MIT'S MAGAZINE OF INNOVATION

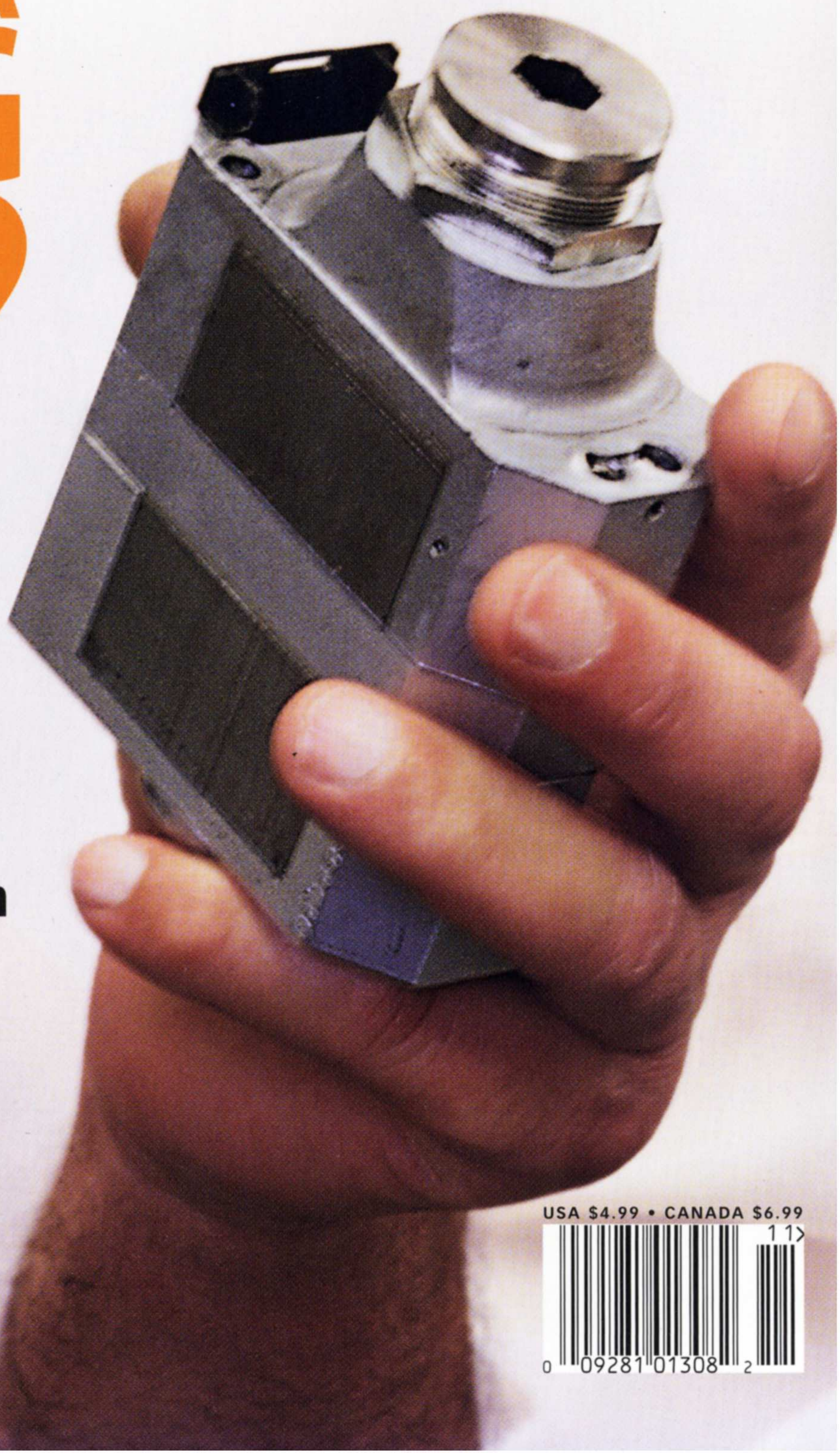
TECHNOLOGY REVIEW

NOVEMBER 2002

WWW.TECHNOLOGYREVIEW.COM

WHY NOT A 40-MPG SUV?

THE TECHNOLOGY IS AT HAND, BUT NO ONE WANTS IT



Holograms in Motion

Personal Genome Sequencing

FBI Cybercrime Crackdown

DIGITAL RIGHTS REPORT

Music and Movies Post-Napster

PLUS

Online Voting Hits Europe

Stomach Pacemakers

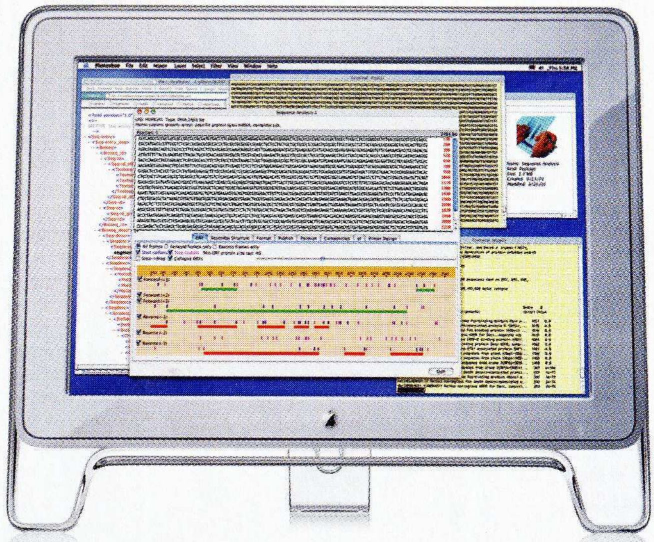
Nano Biomaterials

USA $4.99 • CANADA $6.99

11>

0 09281 01308 2

apple.com/pro



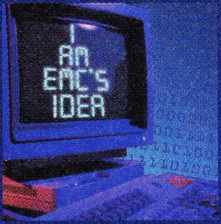
Discoveries.

Genetics researcher Dr. William Gilbert would normally spend the entire day comparing genomes. Then, one day, Dr. Gilbert tried Apple/Genentech BLAST and performed 192 comparisons of two similar genomes, with high word sizes, in less than two hours. Before, he had given up after 16 hours and incomplete results. Now Dr. Gilbert is even using his iPod™ to transfer human genomic data from computer to computer in under a minute. "The network was too slow and it only took 30 seconds using the iPod." Overall, Dr. Gilbert sees profound implications working with Apple: "A/G BLAST will be the most critical tool of the post genomic era by being able to handle larger quantities of DNA sequences at a time."

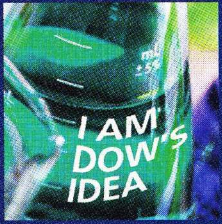
Made on a Mac.

It's not how many ideas you have.
It's how many you make happen.

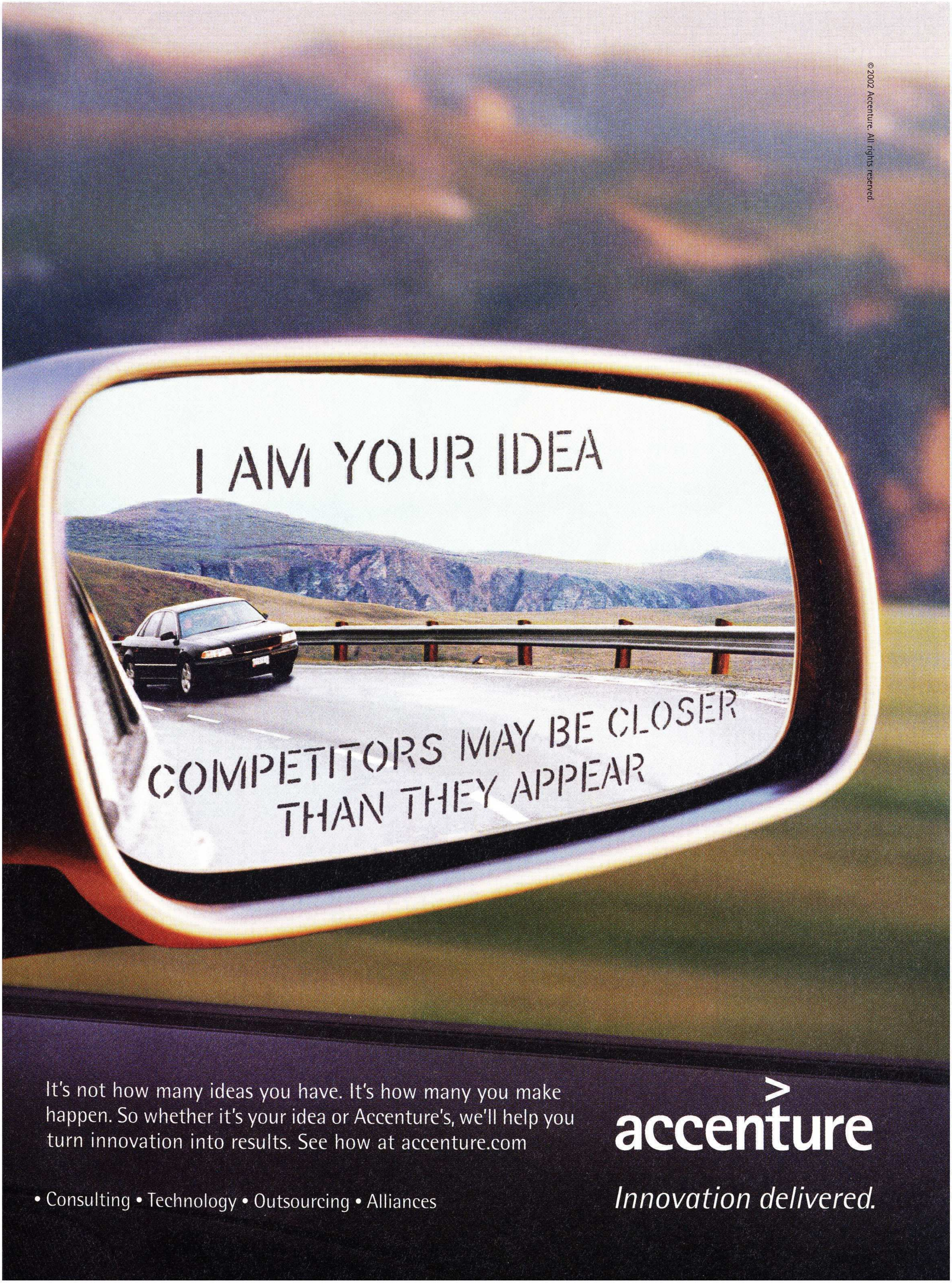
In 1996, after three years of explosive growth but few changes in its operations or business processes, electronics-retailing giant Best Buy's profitability had evaporated and its stock price was plummeting. The company needed a major—and immediate—transformation. **I am Best Buy's idea, delivered.** Best Buy partnered with Accenture to engineer one of the most dramatic success stories in retailing history. In a two-year program applying process, methods and tools that Accenture calls Scientific Retailing, Best Buy increased net earnings 138% and drove its stock price from $2 to $57, increasing its market cap from $403 million to $11.4 billion.

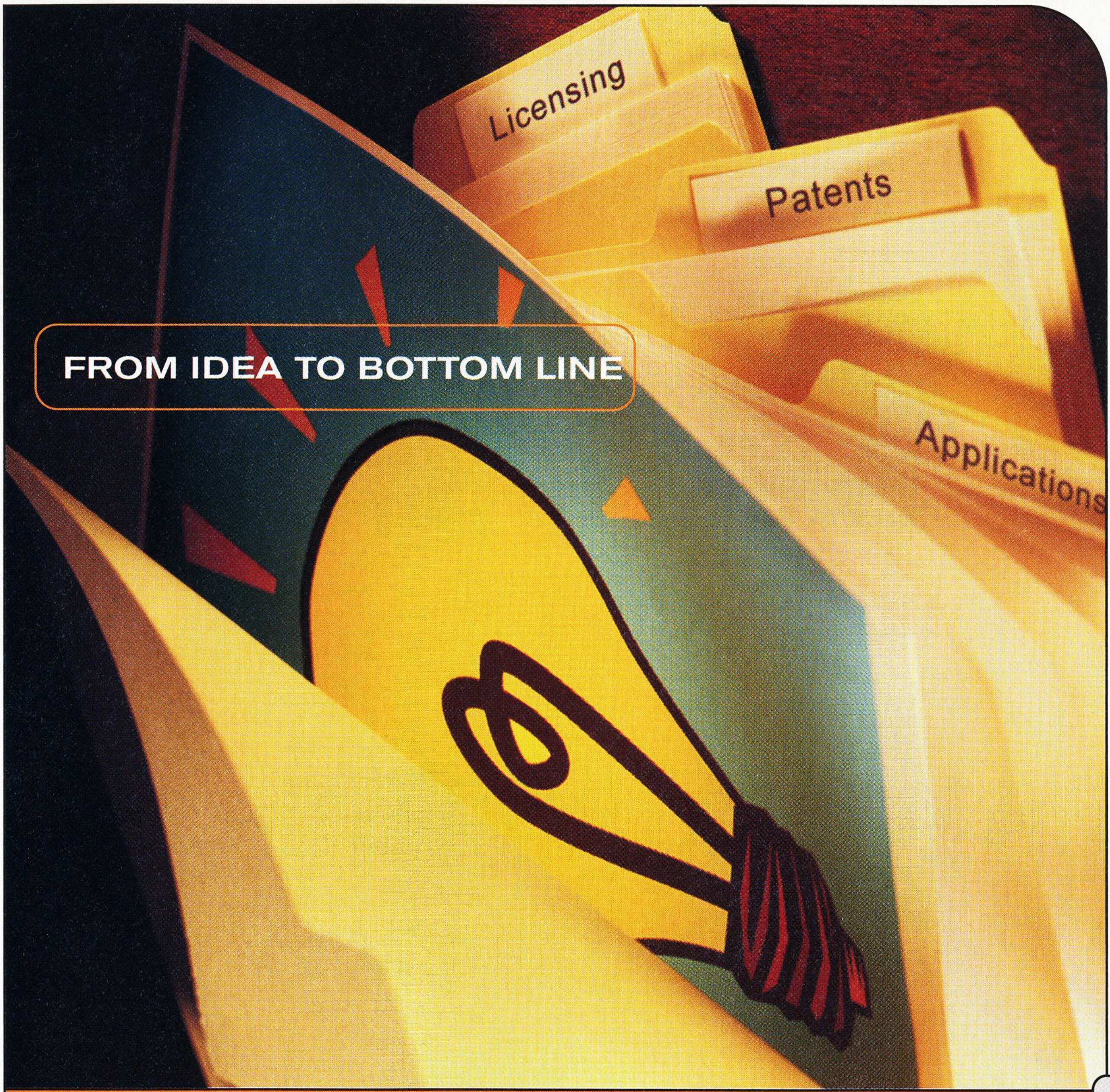


As the global leader in enterprise information storage solutions, EMC recognized that a complete overhaul of its existing business systems was needed to sustain future growth. **I am EMC's idea, delivered.** Accenture teamed with EMC to design and build a massive, scalable information infrastructure to integrate all of EMC's systems and processes globally, accelerate new product introductions and give management more flexibility in responding to changing market conditions. Now, design changes can make the rounds to 6,000 users around the world in minutes, instead of days.



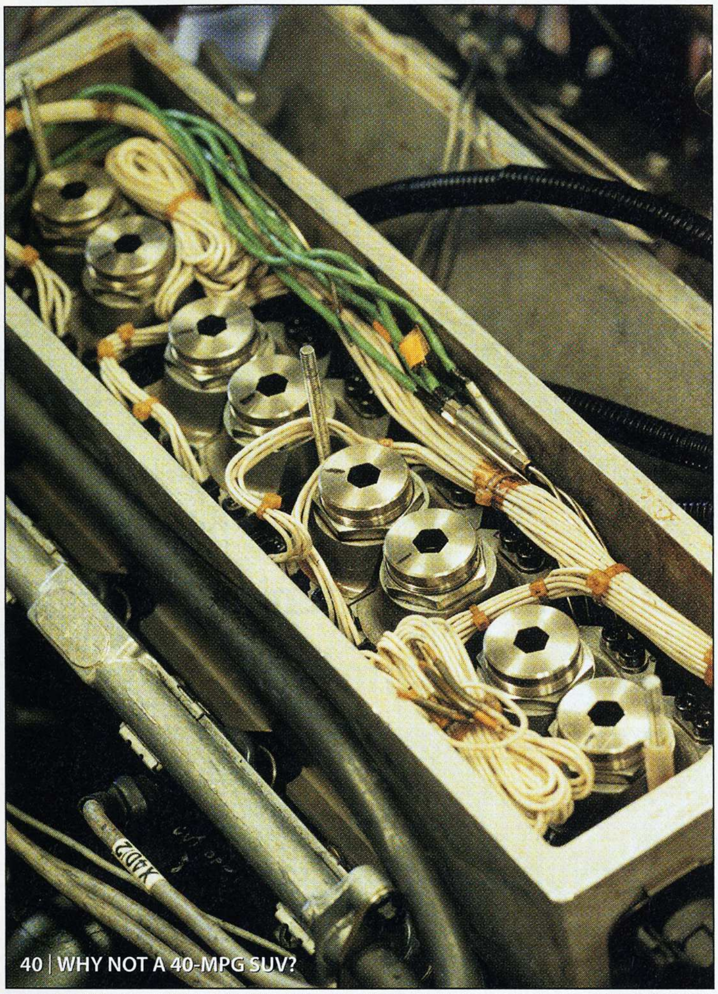
To develop a sustainable competitive advantage in the global chemical industry, Dow sought to aggressively leverage its investment in information technology, dramatically improving systems productivity and significantly reducing application costs and time to market. **I am Dow's idea, delivered.** In a unique outsourcing relationship, Accenture helped Dow consolidate nearly all of its IT activities into four regional centers. Jointly staffed with professionals from both companies, the centers have accelerated time to market by 10%, increased overall productivity by 30% and made a hefty contribution to $70 million in annual IT savings since 1992.


I AM YOUR IDEA
COMPETITORS MAY BE CLOSER THAN THEY APPEAR
It's not how many ideas you have. It's how many you make happen. So whether it's your idea or Accenture's, we'll help you turn innovation into results. See how at accenture.com
• Consulting • Technology • Outsourcing • Alliances
accenture
Innovation delivered.
© 2002 Accenture. All rights reserved.


Licensing
Patents
Applications
FROM IDEA TO BOTTOM LINE

CONTENTS

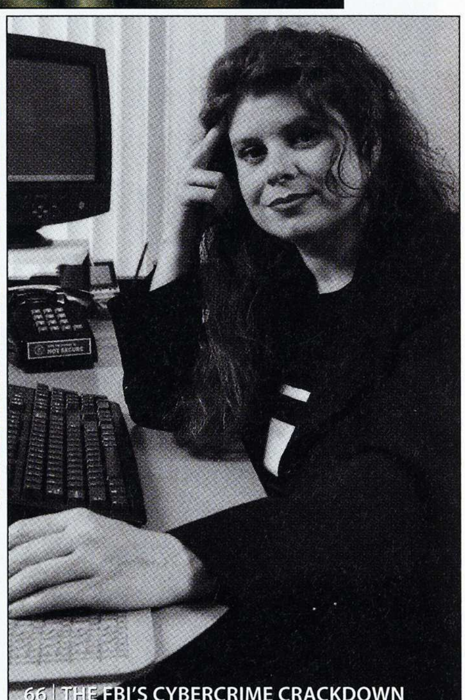
TECHNOLOGY REVIEW VOLUME 105, NUMBER 9



40 | WHY NOT A 40-MPG SUV?

November 2002

48 | HOLOGRAMS IN MOTION

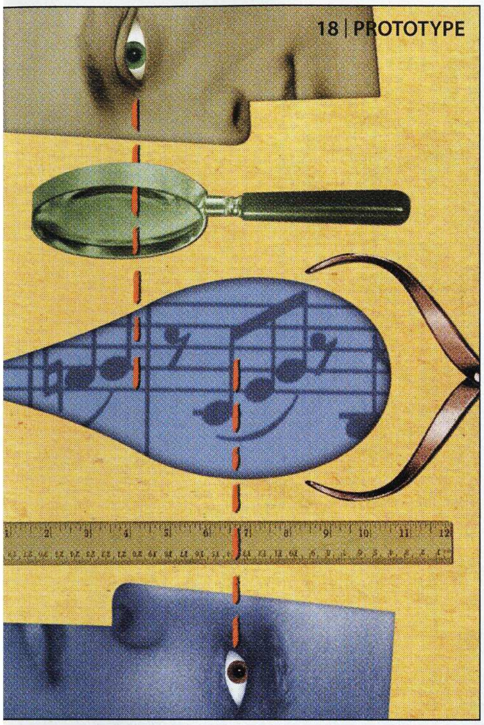


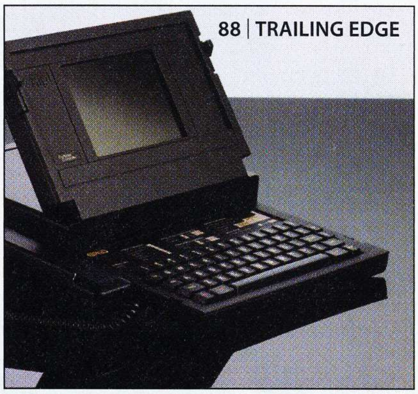
66 | THE FBI'S CYBERCRIME CRACKDOWN

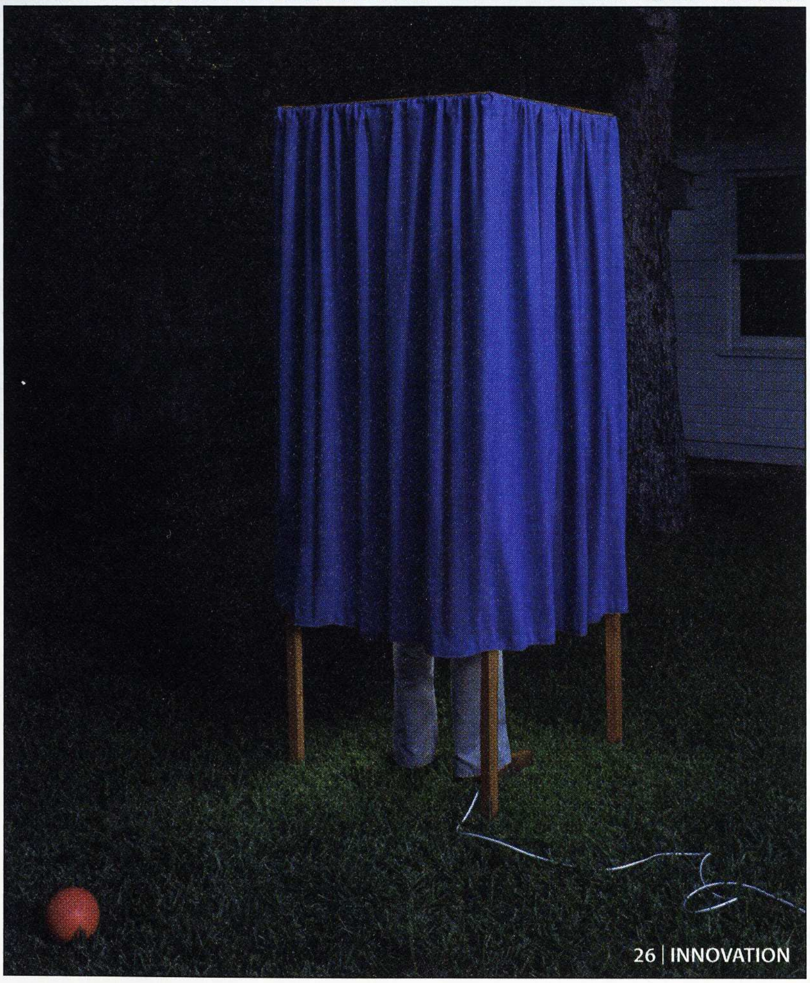
On the cover: Fuel-saving electromechanical valve actuator. Photograph by John Sobczak.

CONTENTS

TECHNOLOGY REVIEW VOLUME 105, NUMBER 9


18 | PROTOTYPE


88 | TRAILING EDGE


26 | INNOVATION

DEPARTMENTS

COLUMNS

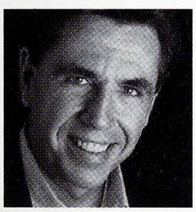
INFORMATION WANTS A FEE

It has become a tenet of the Internet age that information wants to be free. "Information," according to this dogma, encompasses music, movies, and anything else that can be represented by digital bits. Music wants to be free, proclaim the peer-to-peer file-sharers who use the Internet to help themselves to MP3 files of their favorite songs. Movies want to be free, chime in the "cammers" who sneak digital cameras into screening rooms and dump copies of films onto the Web before they have made their official debuts.

But these "truths" are myths. It's more accurate to say that information wants a *fee*.

This twist on the digital-age mantra is the overriding lesson of our special report, "Digital Entertainment Post-Napster" *(p. 56)*. The central problem, our stories make clear, stems from the fact that too many people have extended the meaning of *free* from "let loose" to "let loose without charge." And that is not going to cut it.

Our first piece looks at the technology of making compact discs copyproof—a practice gaining favor with the recording industry as a way to foil pirating. Its companion story concentrates on a lone French hacker, originally known to the world only by his Internet moniker "Gej," who developed what many proclaimed would be the Napster of movies—a way to copy and compress high-quality film images for distribution over the Web. But Gej, whose real name is Jérôme Rota, didn't want to be dogged by lawyers and law enforcement. We found him at his San Diego startup, where he is trying to parlay his compression technologies into a legal and profitable business that will make it easy for us to download and play movies—*after* we've paid for them.



Indeed, as both stories reveal, a grab bag of forthcoming technologies should make sure music and movies continue to be freely available—for a price. On the music front, some approaches target technical differences between the ways audio CD players and computers read and play songs, allowing unlimited and distortion-free listening on the former but introducing unharmonious noise on the latter. Others seek to prevent uncontrolled distribution by restricting the number of times a piece of digital entertainment can be copied.

Not all these technologies make good business sense. Some, such as those that let you to play a legally purchased CD on your home stereo but not on an office computer, are just plain annoying and will be tough sells to consumers. And there are always hackers out there able to break any protection technology that is dreamed up.

But still, get used to it. Such controls are inevitable because that's how things work in a market-driven economy that values intellectual property. Steadily, relentlessly, these technologies will become pervasive. No CD you buy—Bach, Beck, or the Backstreet Boys—will be without some form of protection. The same will hold true for any movie you purchase or download, be it a classic such as *Casablanca* or some future Austin Powers release.

This inevitability does not please everyone. In this very issue, columnist Simson Garfinkel calls the acceptance of digital rights management a deal with the devil *(see "The Rights Management Trap," p. 37)*. Simson says he would rather have his writing ripped off than cede control of what he puts on his computer to such technologies.

The trick, of course, will lie in finding the right balance of fair use and fair compensation—so that for the vast majority of us it's not worth seeking ways around the protection technologies. And then digital music and movies will have the kind of protection long enjoyed by other types of information—from newspapers and books to records, tapes, and many forms of spoken advice—and we'll pay for value received.

We'll pay, because that's the best, fairest, and most realistic way to set the information free. —*Robert Buderi*

MIT'S MAGAZINE OF INNOVATION

TECHNOLOGY REVIEW

EDITOR
Robert Buderi

EXECUTIVE EDITOR David Rotman

DEPUTY EDITOR Herb Brody

MANAGING EDITOR Tracy Staedter

ART DIRECTOR Eric Mongeon

SENIOR EDITORS Sally Atwood, Wade Roush, David Talbot, Rebecca Zacks

WEB CONTENT TEAM LEADER Kevin Hogan

SENIOR ASSOCIATE EDITOR Erika Jonietz

ASSOCIATE EDITORS David Cameron, Alan Leo

ASSISTANT ART DIRECTOR Jamie Kelleher

EDITORIAL ASSISTANT Alyssa Danigelis

COPY CHIEF Elyse M. Friedman

FACT CHECKER Lisa Scanlon

PRODUCTION MANAGER Valerie V. Kiviat

EDITORIAL INTERN Gregory T. Huang

CONTRIBUTING WRITERS

Ivan Amato
Jon Cohen
Peter Fairley
David H. Freedman
Simson Garfinkel
Jeff Hecht
Charles C. Mann
Michael Schrage
Evan I. Schwartz
Seth Shulman
Gary Taubes
Claire Tristram
M. Mitchell Waldrop

CUSTOMER SERVICE/ SUBSCRIPTION INQUIRIES

NATIONAL: 800-877-5230
INTERNATIONAL: 386-447-6352
www.technologyreview.com/custserv/inquiry
Cost $34 per year
Canada residents add $10
Other foreign countries add $30

ADDRESS CHANGES

www.technologyreview.com/custserv/addresschange
MIT Records 617-253-8270 (Alums only)

PERMISSIONS

978-750-8400
www.technologyreview.com/magazine/permissions.asp

TECHNOLOGY REVIEW BOARD

Allan S. Bufferd
Jerome I. Friedman
Alice P. Gast
Bernard A. Goldhirsh
William J. Hecht
R. Bruce Journey
Robert M. Metcalfe
DuWayne J. Peterson Jr.
Ann J. Wolpert

REPRINTS

717-399-1900 ext. 118
technologyreview@reprintbuyer.com
or www.technologyreview.com/customerservice/reprints_permissions.asp

TR RELAUNCH FUND

MILLENNIAL PATRON
Robert M. Metcalfe
CENTENNIAL PATRONS
Steve Kirsch
DuWayne J. Peterson Jr.

TECHNOLOGY REVIEW
One Main Street, 7th Floor
Cambridge MA 02142
TEL: 617-475-8000 FAX: 617-475-8043
www.technologyreview.com

United States Postal Service

Statement of Ownership, Management, and Circulation

1. Publication Title: Technology Review
2. Publication Number: 5 3 5 - 9 4 0
3. Filing Date: 10/1/02
4. Issue Frequency: Monthly
5. Number of Issues Published Annually: 10
6. Annual Subscription Price: $34.00
7. Complete Mailing Address of Known Office of Publication (Not printer) (Street, city, county, state, and ZIP+4): MIT, 77 Massachusetts Ave., Middlesex, Cambridge, MA 02139
   Contact Person: Corrine Callahan
   Telephone: 617-475-8016
8. Complete Mailing Address of Headquarters or General Business Office of Publisher (Not printer): MIT, 77 Massachusetts Ave., Cambridge, MA 02139
9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor (Do not leave blank)
   Publisher (Name and complete mailing address): R. Bruce Journey, MIT, 77 Massachusetts Ave., Cambridge, MA 02139
   Editor (Name and complete mailing address): Robert Buderi, MIT, 77 Massachusetts Ave., Cambridge, MA 02139
   Managing Editor (Name and complete mailing address): Tracy Staedter, MIT, 77 Massachusetts Ave., Cambridge, MA 02139
10. Owner (Do not leave blank. If the publication is owned by a corporation, give the name and address of the corporation immediately followed by the names and addresses of all stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, give the names and addresses of the individual owners. If owned by a partnership or other unincorporated firm, give its name and address as well as those of each individual owner. If the publication is published by a nonprofit organization, give its name and address.)

Full Name	Complete Mailing Address
Massachusetts Institute of Technology	77 Massachusetts Ave. Cambridge, MA 02139

11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages, or Other Securities. If none, check box ☐ None

Full Name	Complete Mailing Address

12. Tax Status (For completion by nonprofit organizations authorized to mail at nonprofit rates) (Check one)
    The purpose, function, and nonprofit status of this organization and the exempt status for federal income tax purposes:
    ☐ Has Not Changed During Preceding 12 Months
    ☐ Has Changed During Preceding 12 Months (Publisher must submit explanation of change with this statement)

PS Form 3526, October 1999 (See Instructions on Reverse)

13. Publication Title: Technology Review
14. Issue Date for Circulation Data Below: July/August 2002 Issue

15. Extent and Nature of Circulation	Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a. Total Number of Copies (Net press run)	370,270	365,391
b. Paid and/or Requested Circulation (1) Paid/Requested Outside-County Mail Subscriptions Stated on Form 3541 (Include advertiser's proof and exchange copies)	277,244	279,000
(2) Paid In-County Subscriptions Stated on Form 3541 (Include advertiser's proof and exchange copies)	0	0
(3) Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Non-USPS Paid Distribution	40,631	45,591
(4) Other Classes Mailed Through the USPS	0	0
c. Total Paid and/or Requested Circulation [Sum of 15b. (1), (2),(3),and (4)]	317,874	324,591
d. Free Distribution by Mail (Samples, complimentary, and other free) (1) Outside-County as Stated on Form 3541	4,557	4,042
(2) In-County as Stated on Form 3541	0	0
(3) Other Classes Mailed Through the USPS	0	0
e. Free Distribution Outside the Mail (Carriers or other means)	939	0
f. Total Free Distribution (Sum of 15d. and 15e.)	5,214	4,042
g. Total Distribution (Sum of 15c. and 15f)	323,088	328,633
h. Copies not Distributed	47,182	36,758
i. Total (Sum of 15g. and h.)	370,270	365,391
j. Percent Paid and/or Requested Circulation (15c. divided by 15g. times 100)	98.39	98.77

16. Publication of Statement of Ownership
    ☐ Publication required. Will be printed in the November 2002 issue of this publication. ☐ Publication not required.
17. Signature and Title of Editor, Publisher, Business Manager, or Owner
    Date: 10.1.02

I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including civil penalties).

Instructions to Publishers

1. Complete and file one copy of this form with your postmaster annually on or before October 1. Keep a copy of the completed form for your records.
2. In cases where the stockholder or security holder is a trustee, include in items 10 and 11 the name of the person or corporation for whom the trustee is acting. Also include the names and addresses of individuals who are stockholders who own or hold 1 percent or more of the total amount of bonds, mortgages, or other securities of the publishing corporation. In item 11, if none, check the box. Use blank sheets if more space is required.
3. Be sure to furnish all circulation information called for in item 15. Free circulation must be shown in items 15d, e, and f.
4. Item 15h., Copies not Distributed, must include (1) newsstand copies originally stated on Form 3541, and returned to the publisher, (2) estimated returns from news agents, and (3), copies for office use, leftovers, spoiled, and all other copies not distributed.
5. If the publication had Periodicals authorization as a general or requester publication, this Statement of Ownership, Management, and Circulation must be published; it must be printed in any issue in October or, if the publication is not published during October, the first issue printed after October.
6. In item 16, indicate the date of the issue in which this Statement of Ownership will be published.
7. Item 17 must be signed.

Failure to file or publish a statement of ownership may lead to suspension of Periodicals authorization.

PS Form 3526, October 1999 (Reverse)

MIT'S MAGAZINE OF INNOVATION

TECHNOLOGY REVIEW

PUBLISHER AND CEO
R. Bruce Journey, bruce.journey@technologyreview.com

VICE PRESIDENT AND GENERAL MANAGER
Martha Connors, martha.connors@technologyreview.com

VICE PRESIDENT, SALES AND MARKETING
Kate Dobson, kate.dobson@technologyreview.com

CORPORATE

DIRECTOR OF BUSINESS DEVELOPMENT
J. R. "Matt" Mattox
matt.mattox@technologyreview.com

HUMAN RESOURCES MANAGER
Ann E. Warner

DIRECTOR OF INFORMATION TECHNOLOGY
Lon Anderson

NETWORK COORDINATOR
Scott Hendry

EXECUTIVE ASSISTANT TO THE CEO
Kelli Talbot

OFFICE ADMINISTRATOR
Eileen Cahalane

OFFICE INTERNS
Walter Rodriguez

TECHNOLOGYREVIEW.COM

CONTENT MANAGER
Kristy Robinson

LEAD WEB TECHNOLOGIST
Eric Engel

GRAPHIC DESIGNER
Matthew Bouchard

CONTENT AND TRAFFIC ANALYST
Thomas Pimental

CONTENT ASSOCIATE
Johanna Purcell

SALES AND MARKETING

ASSISTANT TO THE VP, SALES AND MARKETING
Sharon Morani

ADVERTISING SERVICES COORDINATOR
Amy McLellan
amy.mclellan@technologyreview.com

SENIOR MARKETING MANAGER
Kathleen Kennedy

CONSUMER MARKETING

DIRECTOR OF CIRCULATION AND CONSUMER MARKETING
Elaine Spencer

DIRECT RESPONSE MANAGER
Sharon Maxell

ASSOCIATE CONSUMER MARKETING DIRECTOR
Corrine L. Callahan

CONSUMER MARKETING ASSISTANT
Faith Welt

FINANCE

CONTROLLER
John W. Keegan

SENIOR ACCOUNTANT
John F. Leahy

ACCOUNTANT
Letitia Trecartin

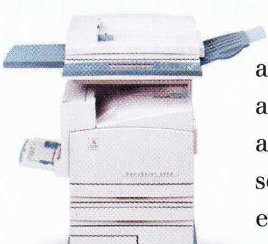
ADVERTISING SALES

NEW ENGLAND/BOSTON: 617-475-8004	Paul Gillespie	paul.gillespie@technologyreview.com
MID-ATLANTIC/NEW YORK: 212-419-2820	Alan Levine Mason Wells Jamie Casale	alan.levine@technologyreview.com mason.wells@technologyreview.com jamie.casale@technologyreview.com
SOUTHEAST/NEW YORK: 212-419-2820	Dean Grant	dean.grant@technologyreview.com
SOUTHWEST/DALLAS: 972-625-6688	Randy Artcher Steve Tierney	randy.artcher@tierney.com steve.tierney@tierney.com
MICHIGAN/DETROIT: 248-546-2222	Colleen Maiorana Sue Scott	colleenm@maiorana-partners.com sscott@maiorana-partners.com
MIDWEST/CHICAGO: 312-629-5264	Chris Svoboda	amssvoboda@aol.com
NORTHWEST/SAN FRANCISCO: 415-659-2980	Merrick Musolf Sam Staley	merrick.musolf@technologyreview.com sam.staley@technologyreview.com
SOUTHERN CALIFORNIA/L.A.: 310-451-5655	Gregory Schipper	gschipper@whiteassociates.com
AUSTRIA AND GERMANY: 49-89-9392-6711	Guido Klausbruckner	gklausbruckner@web.de
AUSTRALIA: 61-2-9929-5929	Anton Gruzman	sthpac@ozemail.com.au
HONG KONG: 852-2516-1001	Wendy Lin	wlin@publicitas.com
EUROPE: 44-207-630-0978	Anthony Fitzgerald David Wright	afitzgerald@mediamedia.co.uk dwright@mediamedia.co.uk
FRANCE: 33-0-14-270-0008	Philippe Marquezy	spacephm@club-internet.fr
JAPAN: 813-3261-4591	Shigeru Kobayashi	shig-koby@media-jac.co.jp
ONLINE ADVERTISING: 212-419-2824	Anne Toal	anne.toal@technologyreview.com

EUREKA

We discovered how to bring down the running cost of color for any office to under 10 cents a page. And that was no accident. Introducing the Xerox DocuColor 2240 and 1632 Printer/Copiers.

There's a new way to look at it.

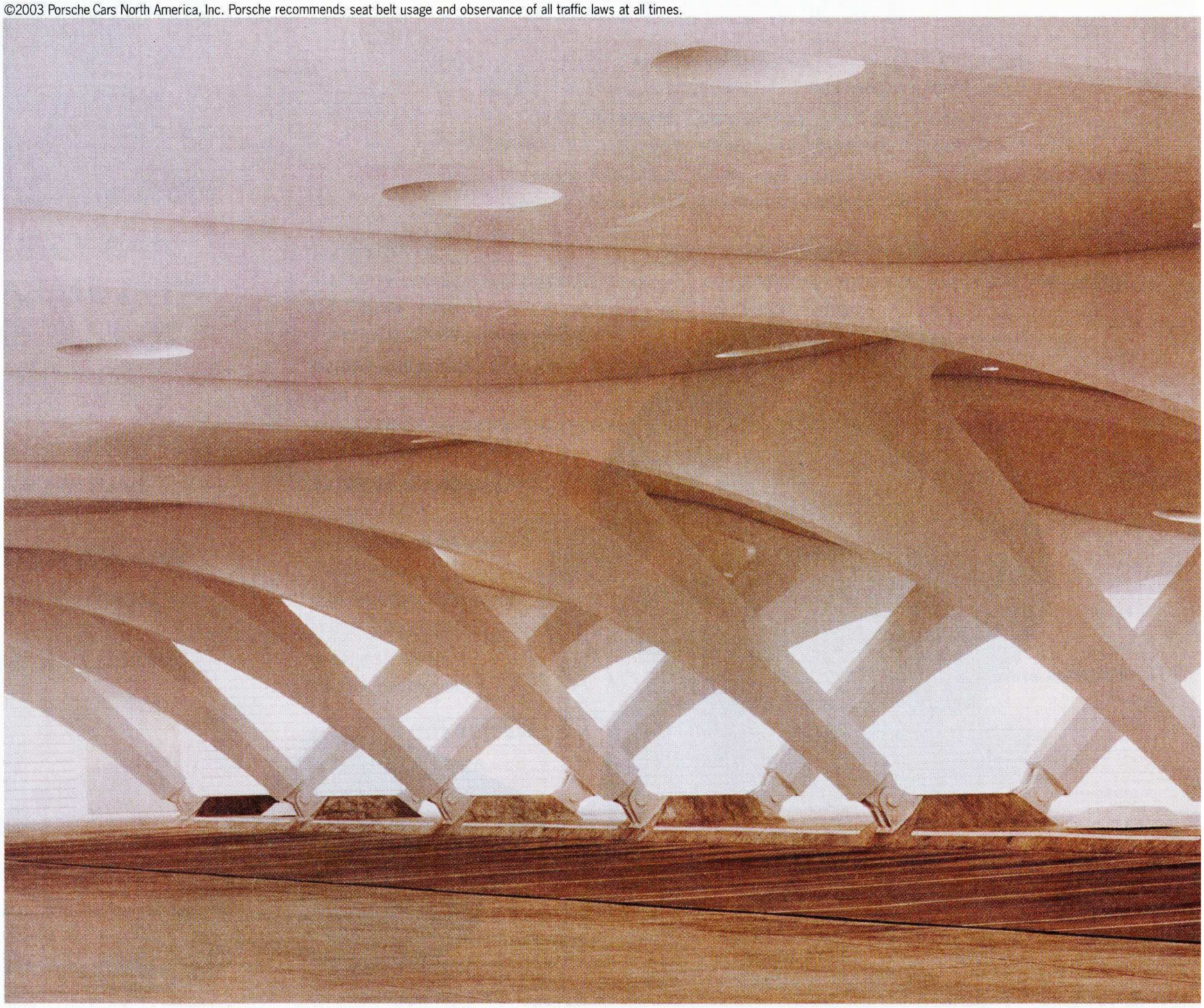


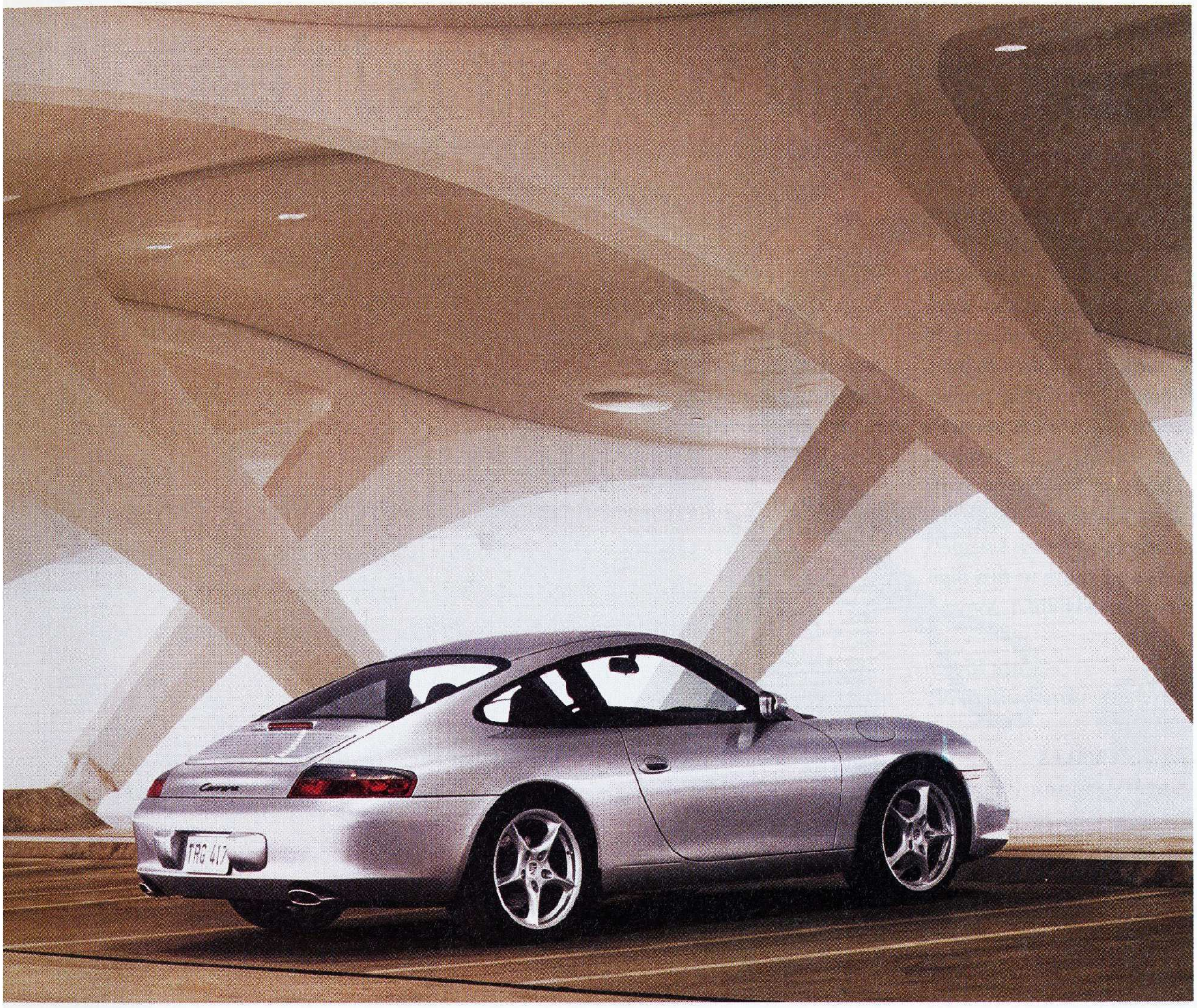
Introducing a dazzling breakthrough in color. The Xerox DocuColor® 2240 and 1632 bring the running cost* of making color prints and copies in your office to less than 10 cents a page. And remarkably, reduce black and white running costs to a mere 1.3 cents a page. So for color and black and white that are easy to use and afford, remember the Xerox DocuColor 2240 and the 1632. Once you discover them, you'll see how simple it can be to integrate color into everything you do. To get all the benefits of low-cost color in your office, get in touch today.

THE DOCUMENT COMPANY
XEROX®

Visit: www.xerox.com/eureka Call: 1-800-ASK-XEROX ext. 2240A

*Per copy charge for service and supplies (excluding paper). Additional charge for equipment lease or purchase and base service applies.




Carrera
TRG 417

DIGITAL THEATERS: COMING SOON?

With regard to the speed with which Michael Hiltzik suggests digital projection will proliferate ("Digital Cinema, Take 2," *TR* September 2002), I think a point is being missed. Once a theater has digital-projection capability, it can show many products, from rock concerts to corporate presentations. In Great Britain, a recent experiment with digital projection of three Broadway-based shows drew rave reviews and commanded premium ticket prices. There are also some fairly big savings to the studios from not having to deliver prints to each theater. I suspect the theater chains may move to this digital medium more quickly than conventional wisdom thinks.

Jack Rivkin
Amagansett, NY

FIRED UP OVER FIREWALLS

Simson Garfinkel's column ("Firewall Follies" *TR* September 2002) should be required reading for upper managers before they sign off on information technology budgets. Firewalls, like other network devices, are not an install-and-forget type of technology. The vast majority of organizations have no idea who made what changes to their network infrastructure or why the changes were made. The poor security methodologies that are standard practice—typically a single, broadly shared password—don't allow for tracking changes. Until this is resolved, the network infrastructure can't be trusted.

Jonathan Wolf
Waltham, MA

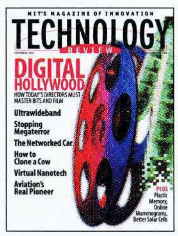
HOW TO HANDLE MEGATERROR

Your article on "The Technology of Megaterror" (*TR* September 2002) is excellent. However, I do not share writer Richard Garwin's belief that we are safe from smallpox. We are not.

Aside from the fact that the general population has not been vaccinated recently, there is the deadly possibility that the Soviets or a subsequent bioweapons-research team has developed mutant versions of the smallpox virus for which the existing vaccine does not work.

Ralph Chang
Arlington, MA

Garwin asserts that radiological dispersal devices "pose limited immediate harm." I disagree. Although it is true that alpha and beta particles contaminating a dust or vapor cloud could easily be removed by hygiene measures, these particles would be extremely toxic and possibly life threatening if inhaled or ingested.



"The poor security methodologies that are standard practice—typically a single, broadly shared password—don't allow for tracking changes. Until this is resolved, the network infrastructure can't be trusted."

To lessen the impact of such an event, an early-warning-and-response system could direct potential victims within range of a contaminated cloud plume to remain indoors so that they would avoid inhalation. Homeowners could deploy "safe rooms" sealed with material as simple as plastic and duct tape or use self-contained breathing apparatuses to protect themselves from exposure. In addition, the filtration and positive-pressure systems recommended for protection against bioterrorism could be leveraged to mitigate the effects of radiological dispersal. Buildings or office clusters could be identified for sequestering members of the traveling public until they could be evacuated, or relocated.

William F. Mead
U.S. Search and
Rescue Task Force
Elkins Park, PA

PUSH HERE FOR INNOVATION

The suggestions in Michael Schrage's column, "Push-Button Innovation" (*TR* September 2002) are good, but he neglects one crucial element: voice controls to bypass those tiny keyboards altogether. Voice recognition would go a long way to making the cell phone easier to use. Tie in a way to record voice memos and parts of a phone conversation. Use it to convert your voice to a text message for e-mailing.

The phone is supposed to be about verbal communication. Make its control verbal, and you've got a real innovation people will appreciate.

Steve Jordan
Germantown, MD

WHO FIRST TAMED THE SKIES?

I read the recent article on Glenn Hammond Curtiss ("The Flight That Tamed the Skies" *TR* September 2002) with great interest. However, I was surprised to see the claim that the NC-4 aircraft designed by him was the first to successfully cross the Atlantic in 1919. We in Great Britain are taught that this honor fell to the Vickers Vimy, piloted by Sir John Alcock and Arthur Brown.

John Steedman
Winchester, England

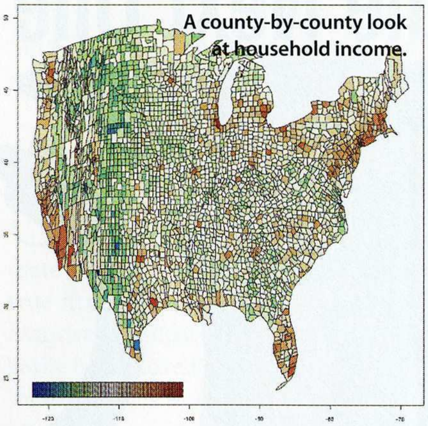
Editor's response: Alcock and Brown were first to fly nonstop across the Atlantic Ocean. Curtiss's seaplane made the trip in several hops.

CONTACT US

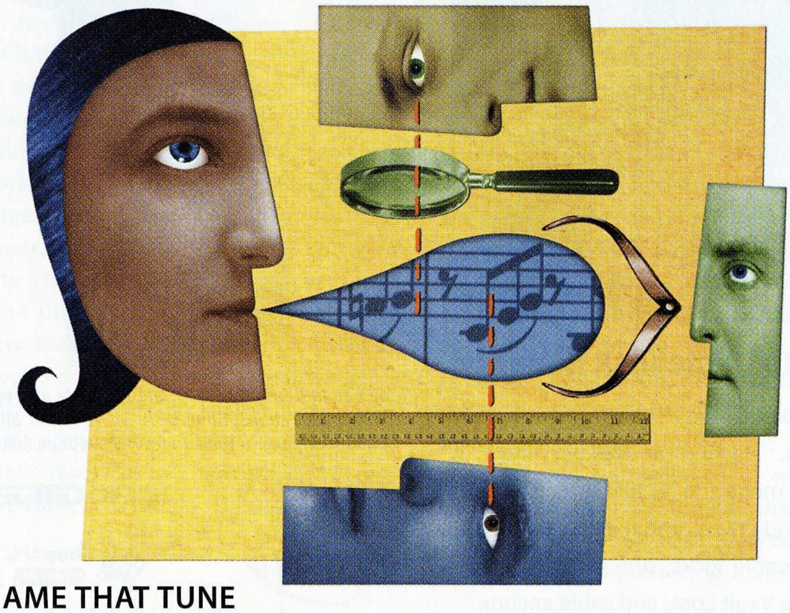
WRITE: ***Technology Review*, One Main Street, 7th Floor, Cambridge MA 02142**
FAX: 617-475-8043
E-MAIL: letters@technologyreview.com.

- **Please include your address, telephone number and e-mail address.**
- **To participate in our online forums, visit www.technologyreview.com and click on "Forums," in the menu at left.**
- **Letters may be edited for clarity and length.**

DATA MAPPING


A county-by-county look at household income.

Pollsters, public health officials, and marketing executives are among the many who use cartograms, special maps that provide a visual sense of geographic information by distorting it in proportion to a key variable. Researchers at AT&T labs in Florham Park, NJ, have created software that takes just minutes to calculate the distortion for thousands of regions (say, for all 3,066 U.S. counties), while old methods could take hours and could handle only tens of regions at a time. The AT&T technology reduces the computational job by imposing lines of various lengths and orientations across the map and performing size adjustments to the space on either side of each line. The process reconfigures geographic regions into recognizable but meaningfully transformed shapes without having to recalculate the whole map. Earlier cartogram programs used different approaches: Some treated the regions like balloons that inflated or deflated in a process that worked quickly but didn't preserve recognizable shapes. Other software that treated the data as a series of mathematical equations produced more familiar and accurate shapes, but consumed hours of processing time. Daniel Keim, the new software's lead developer, says AT&T began using it this year and researchers are refining it while the firm pursues licensing agreements.



NAME THAT TUNE

Forget the name of a song you heard on the radio this morning? Soon, thanks to an audio search engine developed by researchers at Philips Electronics in Eindhoven, the Netherlands, you will be able to search a database and find the song simply by humming its melody. A specialized device embedded in either a desktop computer or a compact disc player will capture your voice, and algorithms will identify the duration and pitch of each note in the song's melody, creating an audio fingerprint. The fingerprint will then be fed into a search engine that uses pattern recognition software to find a matching song stored on a compact disc, computer hard drive, or even the Internet.

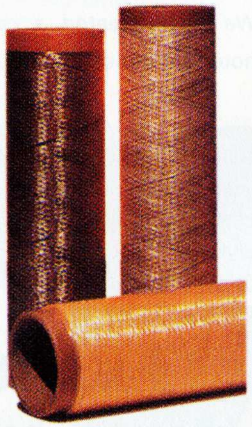
Other audio-search engines in development might not work well for people who are even slightly tone deaf, but Philips's technology works for people with musical training and "people who can't sing, like myself," says Boris de Ruyter, a senior scientist at Philips. The company hopes to market the technology in consumer products within two years.

FEEL-GOOD DRUG MAKING

A system that lets researchers touch, feel, and prod 3-D molecular images could improve scientists' sense of how molecules interact, aiding the development of new drugs. Texas A&M University biochemist Edgar Meyer and his colleagues Stan Swanson and Jennifer Novak are developing simulation software that will make just such a system possible. Their software calculates millisecond-by-millisecond changes in the behavior of the interacting molecules; a commercially available joystick-like interface translates that 3-D information into a tactile sense of pushing, pulling, or resistance. Because many therapeutic agents work by binding tightly with disease-causing molecules, the software could be a critical tool that allows researchers to virtually check—and modify—the fit between molecules. Meyer plans to partner with one or more pharmaceutical companies within the year.

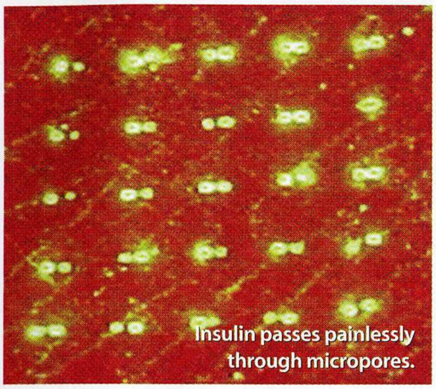
ELECTRIC WEAVE

DuPont researchers have developed a flexible textile that conducts electricity. The advance could facilitate the seamless incorporation of electronic devices into clothing. Each fiber of the new textile consists of a core of DuPont's ultrastrong polymer Kevlar covered with a layer of electrically conductive material such as silver or nickel. Bundles of these fibers are coated with a second polymer for protection during washing. Although many textiles for wearable electronic devices are under development, the DuPont material is the first that combines high electrical conductivity with flexibility sufficient for weaving and embroidery. DuPont's fiber is now commercially available and was recently used by a Finnish sportswear company to make a prototype cold-weather survival suit—complete with an embedded heart monitor, a body-temperature sensor, and a Global Positioning System device.


Kevlar-based fibers could charge up clothes.

COURTESY OF DUPONT (ELECTRIC WEAVE); JOYCE HESSELBERTH (ILLUSTRATION); COURTESY OF AT&T (DATA MAPPING)

HEAT TREATMENT

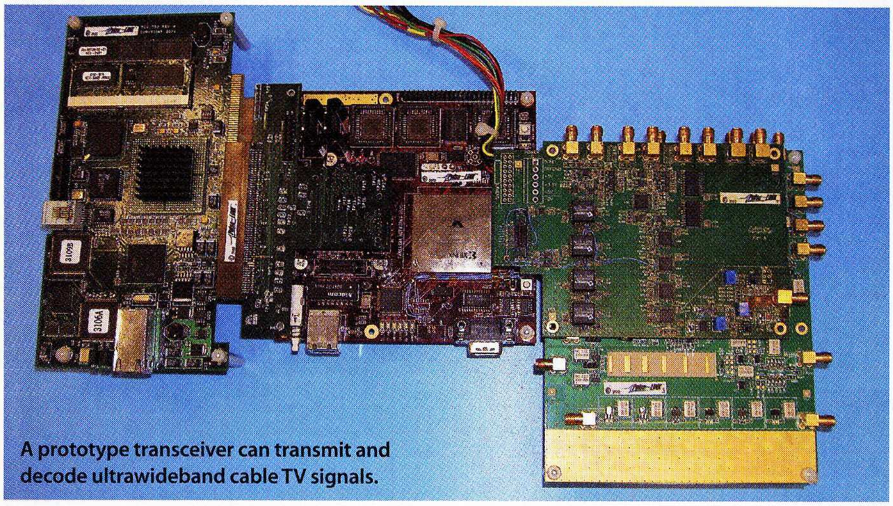


Insulin passes painlessly through micropores.

Atlanta-based Altea Development is creating what has long been a diabetic's fantasy: a system that delivers insulin through skin patches rather than by injection. First the patient places on his or her skin a handheld device bearing an array of tiny filaments. Each of the filaments delivers a three-millisecond burst of heat that vaporizes dead and dying cells and creates a micropore in the skin's outer layer, which normally blocks absorption of large molecules such as insulin. Because the pulse of heat is too brief to affect the underlying living cells, the process is painless. The patient can then replace the device with an insulin-filled patch; for the next 24 hours, the insulin diffuses into the skin and is absorbed into the bloodstream. Alan Smith, Altea's vice president of research, says that preliminary tests with human subjects have been successful, and he expects more extensive clinical trials to begin by the end of this year.

TINY NUKES

Amit Lal is looking for power—in doses small enough to run microscopic machines. The Cornell University electrical engineer and his colleagues have found a way to use nuclear energy to power such microelectromechanical systems as those used for sensing or communications. Making batteries small enough to work with microscopic machines has been a challenge, but a speck of radioactive material, says Lal, could power such a device for more than 75 years. Lal's system comprises a tiny copper cantilever that hovers above a thin film of radioactive nickel. The nickel emits electrons that hit the tip of the cantilever, causing it to deflect and swing back. This cyclical motion could be used to move a second mechanical component, or to generate electrical current. Using that current, nuclear-powered sensors embedded in the walls of buildings could run autonomously for decades, says Lal. He and his Cornell colleagues have started a company called Lifesonics in Ithaca, NY, to commercialize the technology. Lal hopes to have a prototype nuclear-powered temperature-and-pressure sensor ready within two years.



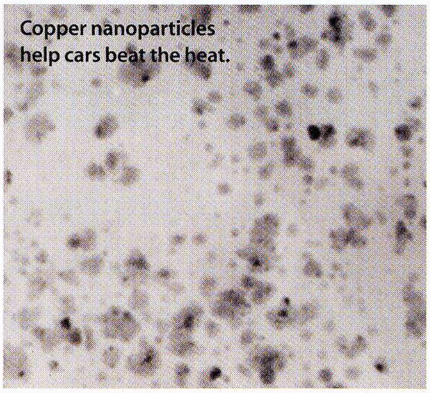
A prototype transceiver can transmit and decode ultrawideband cable TV signals.

THE PULSE OF CABLE

Ultrawideband technology, which uses timed pulses to transmit data, is rapidly emerging as a breakthrough in wireless: it provides the possibility of sending more data faster than any alternative. San Diego startup Pulse-Link wants to make ultrawideband the hot new technology for cable television as well. Requiring no changes to existing cable-television infrastructure, Pulse-Link's system calls for as little as one new piece of equipment at the cable company's facility and an additional user-installed box in each subscriber's home. Pulse-Link's equipment can encode and decode data that are sent in approximately nanosecond-long pulses and spread across all the radio frequencies used by standard cable television. This technology, which won't interfere with conventional signals, should double the amount of information that can be sent over the cables and allow cable operators to deploy bandwidth-hogging high-definition television signals without giving up existing channels.

COOLER CARS

Today's hefty automotive cooling systems, which can barely keep up with the heat produced by our car engines, may be inadequate for cooling the more demanding hybrid and fuel-cell vehicles of tomorrow. For a boost in cooling power, Stephen Choi and his team at Argonne National Laboratory have added nanometer-size copper particles and carbon nanotubes to radiator fluids such as ethylene glycol. Because the solid particles conduct heat a thousand times better than most liquids, researchers have been dreaming of such liquid-solid mixtures for decades. But it is only recently that they've been able to create particles small enough that they don't settle out of the fluid or abrade engine blocks. So far these nanofluids have demonstrated more than double the cooling capacity of typical coolants; that could translate into smaller, lighter cooling systems and better gas mileage. Argonne is partnering with several companies to develop a cheap means of producing the nanoparticles and hopes to bring nanofluids to market within five years.



Copper nanoparticles help cars beat the heat.

COURTESY OF APPLIED PHYSICS LETTERS (COOLER CARS); COURTESY OF PULSE-LINK (PULSE); COURTESY OF JONATHAN EPPSTEIN (HEAT)

A small pharmaceutical company had outsized ambitions: to grow quickly into a global powerhouse. Morgan Stanley helped make it happen. First by searching out the most strategic merger partner. Then brokering sensitive negotiations to create

Services offered by Morgan Stanley & Co. Incorporated, member SIPC. Employee names have been changed to protect their privacy.

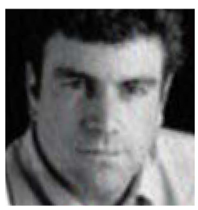

00000070
Diabetes Trials

SCRATCHING A NICHE

A major U.S. financial institution—call it HugeBank—was justly proud of the innovative online services it offered its millions of customers. It finally got around to analyzing its virtual customer base. The findings stunned management. Roughly 90 percent of the bank's online customers logged on barely once a month. By contrast, an obsessive-compulsive 10 percent logged on at least once a day. HugeBank was both embarrassed and annoyed that its pathological dependence upon averages had led it to create a "typical customer," concealing the extent of this disparity.

But here's the steel-toed kicker: that laggard 90 percent accounted for barely 30 percent of the bank's deposits; the hotwired 10 percent accounted for almost 70 percent of the money. In other words, HugeBank's most valuable customers by far were those who embraced the online service.

Those stark statistics obliterated what had once been a broad and aggressive innovation agenda filled with Internet-based strategies. The bank discovered that "Internet innovation" had completely different meanings—and profit potentials—for each of these customer segments. The bank's belief that a single new-product development group could create cost-effective innovations for all the company's customers provoked a huge internal debate that continues to this day.



With apologies to Harvard Business School's Clayton Christensen, this revelation represents the innovator's real dilemma: innovation *for whom?* It's not obvious which of these customer segments merits what kinds of innovation. Should the bank focus its technology initiatives on better service for its nebbishy 90 percent or for its most opulent top tenth? A solid business case could be made that the bank would be better off investing the barest minimum to support the 90 percent. Then again, the bank had best be careful about how innovative it should be with the most active customers. They may want less online innovation, not more. Indeed, they may not want innovation per se: they may simply want better service.

But within that top 10 percent of active customers lurk even more provocative questions: Could there be a 10 percent subset that accounts for a similarly disproportionate amount of online usage and bank assets? And might this elite 1 percent become even more valuable if it were offered even newer online offerings?

Economically successful innovation requires economically successful segmentation. Segments that generate growth often require innovations that are fundamentally different from those offered to segments that generate profits. Pharmaceutical companies manage innovation one way for doctors who write prescriptions and another for the HMOs that manage the finances.

While there is no question that the future of segmentation and the future of innovation are increasingly intertwined, strategic innovation generates a portfolio of questions about innovators' desire to service the segments that matter and ignore those that don't. Most innovators could afford to invest far less creative effort on improving their innovations in favor of investing more ingenuity in finding customer segments that matter. That's what HugeBank is now doing. The pleasant surprise? Improving the segmentation enhances the innovation. The needs of that 90 percent become clearer; the trends for that vital 10 percent stand out.

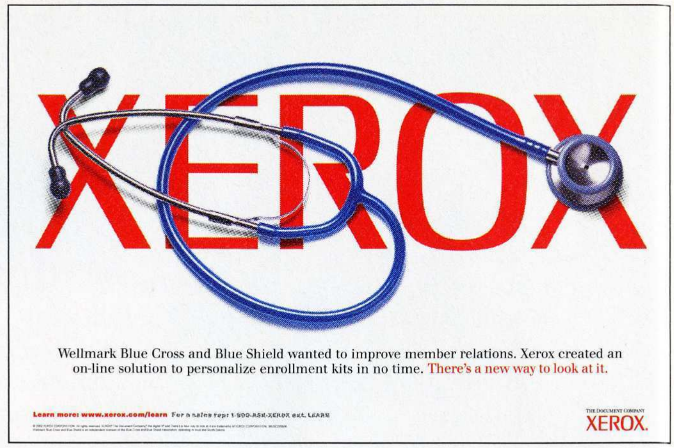
So a most intriguing aspect of a digital medium such as the Internet is that it turns the traditional practices of marketing inside out. Ordinarily, innovative companies spend lots of management time and effort identifying key customers and defining strategic market segments. But as the HugeBank anecdote demonstrates, the rise of Internet-based product and service innovations gives customers the opportunity to unconsciously segment themselves.

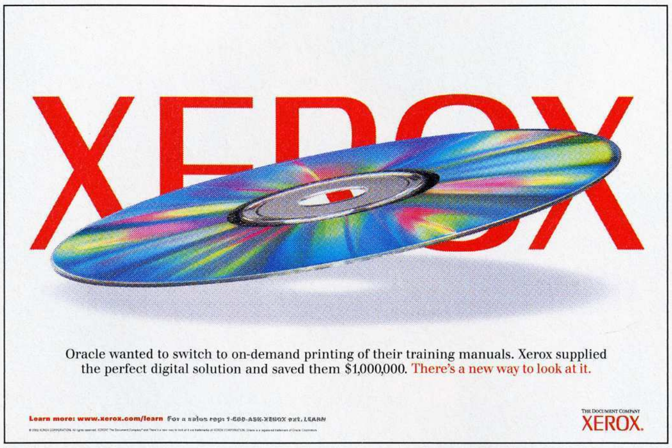
Successful innovation requires successful segmentation. Pharmaceutical companies manage innovation one way for doctors who write prescriptions, another for HMOs that manage finances.

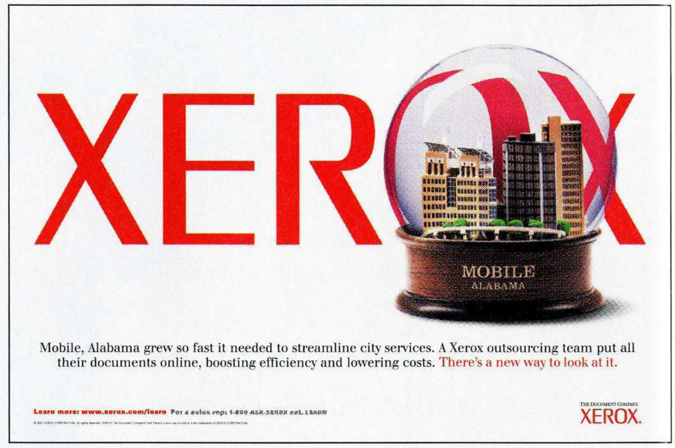
This change should mean a marketing revolution for savvy innovators. Instead of shepherding their customers into predefined market segments, innovators can creatively leverage digital interactions to enable customers' cost-effective self-segmentation. In other words, instead of spending money to sort out customers, spend money to let customers do it themselves. More often than not, the economics and insights that are derived from self-segmentation prove more favorable than traditional approaches. HugeBank has discovered that it's cheaper to model services that are based on how customers actually bank online than it is to design new products and marketing campaigns that attempt to change customers' behaviors.

The fact is, network economics allow innovators to outsource the vital market-segmentation function. That makes targeted innovation initiatives even more cost-effective. The business challenge is to pick the right segments. Should innovators follow the money? Can they afford to underinnovate or underinvest in what might be the segments of tomorrow?

To be sure, some business pundits believe that the ultimate destiny of segmentation is personalization and that technology will transform mass production into mass customization. Perhaps it will. But in the final analysis, customers have as many traits and preferences in common as they do differences. Market differentiation emerges from the differences, but economies of scale emerge from the commonalities. The economics of segmentation will drive tomorrow's economics of innovation. TR

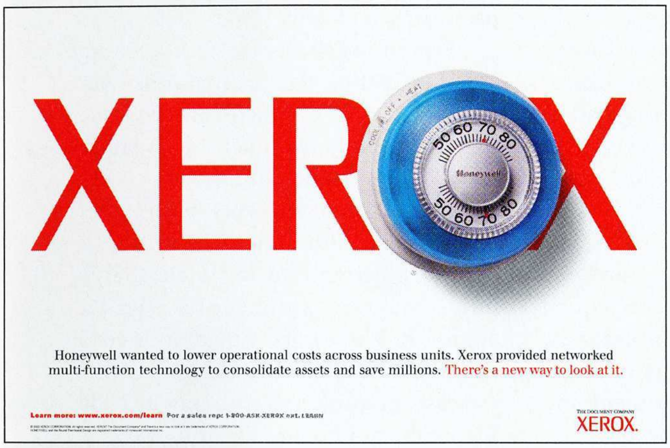


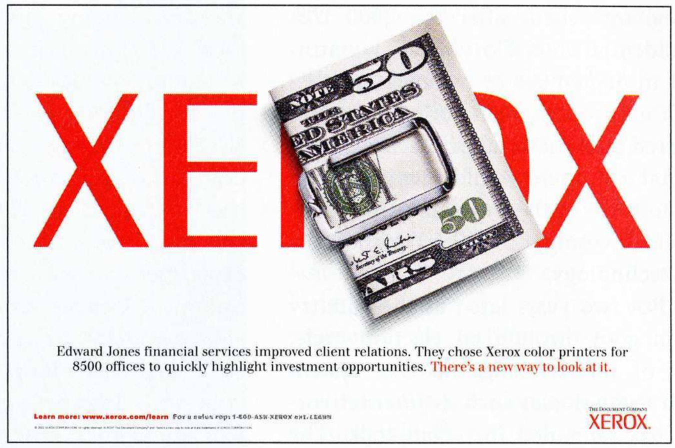


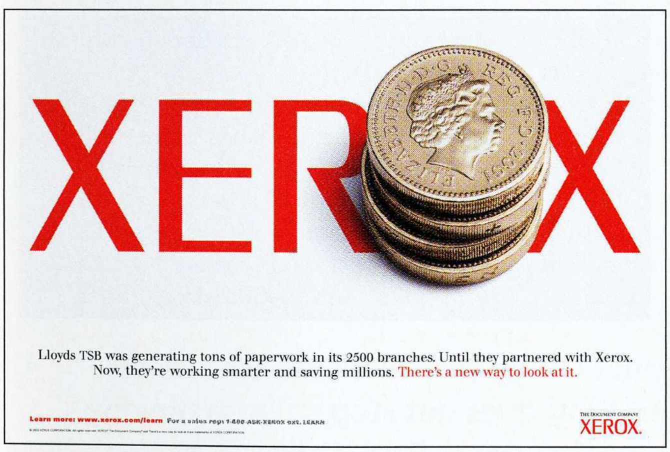


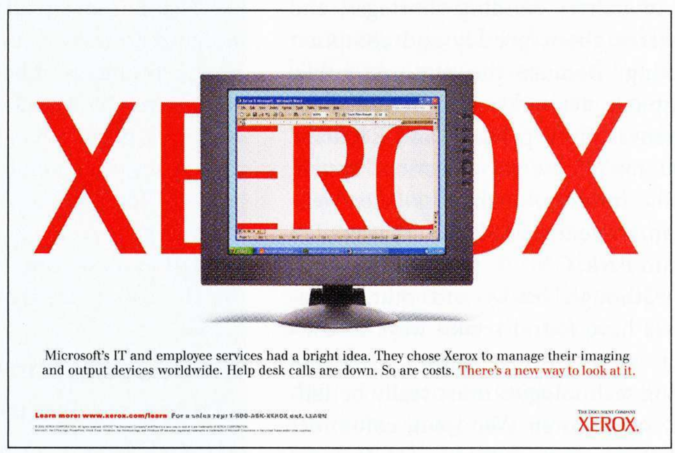
If you're looking for better ways to improve all your network printers, one name bears

Learn more: www.xerox.com/learn For a sales rep: 1-800-ASK-XEROX ext. LEARN









work flow, or cut operating costs, or manage repeating. There's a new way to look at it.

THE DOCUMENT COMPANY
XEROX®

VENTURING TO VOTE ONLINE

European governments experiment with Internet elections

Who will ever forget the endless examinations of Florida's paper ballots and the debates over "hanging" and "pregnant" chads after the 2000 U.S. presidential vote? Florida's saga continued in September as technical glitches with new touchscreen voting machines marred gubernatorial primaries. In this digital age, there would seem to be an obvious fix to the problems created by Florida's voting machines: Internet voting technology.

But two years later, as the country again goes through an election cycle, talk of modernizing the U.S. system with technologies such as Internet voting has remained just that—talk. The inaction, experts say, is largely a product of inertia, funding shortages, and concerns about privacy and computer hacking. Because the nation's public computer networks were designed for openness, not privacy and security, "you can't trust any [election] system on the Internet," maintains Peter Neumann, a scientist at SRI International in Menlo Park, CA.

Although banks and other businesses have found secure ways to conduct transactions online, Internet voting technologies must really be failsafe, says Lauren Weinstein, cofounder with Neumann of People for Internet Responsibility. "Banking online has a lot of holes, but when there is an error, it will be revealed." He explains that customers notice problems on their credit card statements, and they receive a reminder if a bill goes unpaid. Voters, on the other hand, usually have no way to check whether their vote was recorded correctly.

Yet Internet voting is making headway in Europe, where national and municipal governments are pushing ahead with multimillion-dollar projects. "There are issues," says Paul Waller, director of e-democracy in the United Kingdom's Office of the e-Envoy, a cabinet office that puts government services online. "[But] the fact that they exist does not stop us from moving ahead and doing lots of research." In local elections last May, the United Kingdom conducted 16 pilot programs that involved voting or counting ballots electronically. Last year, the Swiss government launched a $20 million initiative to develop electronic voting systems. Three cantons, or states, are experimenting with e-voting, and the canton of Geneva says Internet voting will be available to its citizens next year on a trial basis. Italy, too, is testing a large-scale Internet voting system and will publish a report assessing the experiment early next year.

The European pilot programs are designed to test solutions to a number of the problems inherent in Internet voting, from confirming the identity of voters to guaranteeing voters' privacy and protecting online systems against hackers. Identifying voters so that no one can gain access to another person's login and password information and thereby vote more than once is one of the biggest challenges. Geneva officials sent each voter a card with a 16-digit code and six alphanumeric characters under a scratch-off seal; to vote online, residents entered the codes along with their birth dates and municipalities of origin. Because the cards arrive by mail and voters get new codes for each election, large-scale fraud is difficult, according to Michel Chevallier, the project's communication manager.

Italy expects to use smart cards to identify voters. Plans are already in motion to replace Italians' national identity cards over the next few years with cards that include a silicon chip that stores personal identification data. A Milan-based partnership sponsored by the European Commission is building an online voting system that will allow Italians to pass their cards through electronic readers, enter their passwords, and vote.

Preventing hackers from gaining access to voting data as it travels over the Internet is another concern, one that banks and e-commerce companies such as Amazon.com know well. Geneva's system encrypts both votes and voters' identities to make in-transit data impenetrable to intruders; Italy's pilot program is using a similar approach. The United Kingdom is considering a different twist: each voter in a test district would receive a unique code for each candidate. Even if hackers intercepted voting data, they would not know how to interpret the codes or adjust them to alter election results, explains Waller.

Once votes arrive and are finally recorded in a central database, they still need protection from hackers who might steal information on who voted for whom or tamper with results. The plan in Geneva is to separate people's identifying information from their votes and scramble the order of the votes, making it "impossible" to trace how people voted, according to Chevallier. "Safety procedures never link a voter and the content of his or her vote," he says.

U.S. inaction on Internet voting puzzles some Europeans. "There are issues, [but that] does not stop us from moving ahead," says the United Kingdom's Paul Waller.

Critics, however, say that the same techniques that safeguard privacy and anonymity can make it difficult to review election results in the case of irregularities. Conventional voting that uses paper ballots, punch cards, optical scanning, and mechanical lever

FREDRIK BRODEN

machines guarantees anonymity and also leaves a paper trail that officials can later follow; e-commerce and online-banking transactions also generate copious records. But electronic votes can be altered without leaving any sign of tampering. "There is a conflict between anonymity and auditability," says MIT computer scientist Ronald Rivest, who is researching the problem.

Indeed, some experts question whether the early results in Europe add up to real progress toward Internet voting. The European tests have involved "inconsequential elections," says Paul Herrnson, a professor of government and politics at the University of Maryland. "I don't view that as momentum." Herrnson believes it will take years to overcome the technology and policy hurdles to Internet voting.

But if the U.S. Congress approves a pending bill that would give state and local election agencies billions of dollars for new voting technologies, the momentum could pick up quickly. At least two startup companies, VoteHere in Bellevue, WA, and Election.com in Garden City, NY, say they're ready to help U.S. state and county governments conduct public elections. And online voting in the United States already has gained a foothold in the armed forces: service members around the world were able to vote over the Internet in the 2000 presidential election. "Once the door is open through the military, [Internet voting] is just going to continue. Within 10 years we should have a decent system," predicts MIT political scientist Stephen Ansolabehere.

As voters in this November's elections face old-fashioned paper ballots, lever machines, and punch cards, the future of Internet voting in the United States remains too close to call. But Ansolabehere, for one, believes change is likely. And in the end, he predicts, it won't be driven by academics or policymakers, but by beleaguered U.S. election commissioners who see how much Internet voting could simplify their jobs.—*Julie Claire Diop*

TODAY

TOMORROW

TOYOTA

PHONES FAN OUT

MOBILE COMPUTING | Soon anyone with the latest cell phone will be able to check Grandpa's heart monitor, seek a diagnosis of that rattle under the hood, or make sure the hot tub is hot enough. That's because phones now coming onto the market can plug into sensing devices—from health monitors to automotive diagnostic units—to run software that reconciles a hodgepodge of data formats and translates the data for uploading onto wireless networks and the Web.

"The phone is becoming what I call a 'digital Swiss Army knife,'" says Tony Hillman, a technology manager at Sun Microsystems, which has developed one of the software standards turning up in the new phones. "By downloading different applications you can transform [your phone] into a different kind of device," he says.

VTTi of Moss Beach, CA, is one of the first U.S. software companies to cast phones as wireless data gatherers. The company recently used Sun's Java software, for example, to develop a remote automotive-diagnostics program. A Motorola phone running the program can be plugged into the diagnostics port under the dashboard of most cars, says VTTi vice president of engineering, Tim Clark. The phone converts engine data into packets that can be uploaded to a wireless data network operated by Nextel. The data then go to a central Web server where other Java software turns the information into a Web page that can be viewed by mechanics back at the garage.

Future versions of the VTTi system will work with other phones and with networks being built by other wireless providers, Clark says. On the home front, spa owners can use a similar program to check their tubs' water temperature and chemistry data, and they can also send the data to a Web page where they or technicians can turn up the heat or start the whirlpool jets.

VTTi also offers a phone program that sends electocardiogram data from wearable heart monitors directly to medical professionals. In the future, Clark says, similar software could provide a standard way for ambulance operators to upload such data to hospitals, preparing physicians for a patient's arrival. Try doing that with your Swiss Army knife. —*Wade Roush*

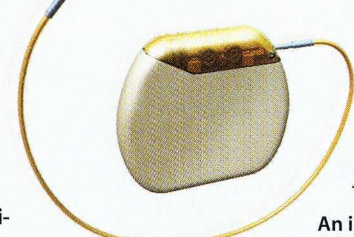
STOMACH PACEMAKER

MEDICINE | Almost 40 million U.S. adults are obese, according to the Centers for Disease Control, and this year some 70,000 of them will go under the knife to have their stomachs bypassed or stapled in painful and expensive procedures that prevent overeating. But if human trials now under way in the United States pan out, overweight people may one day have a less invasive surgical option: a device that helps people feel full by stimulating the stomach with electricity in much the same way a pacemaker stimulates the heart.

The device, under development by Transneuronix of Mount Arlington, NJ, consists of a long flexible wire attached to a pocket-watch-size metal case that contains a battery and an electronic controller, says Steve Adler, Transneuronix vice president. In a brief procedure that could be performed on an outpatient basis, doctors laparoscopically implant the electrode-bearing wire into the muscle around the stomach and insert the case under the patient's abdominal skin. When the device is activated two weeks later, it begins to deliver high-frequency electrical pulses to the patient's stomach.

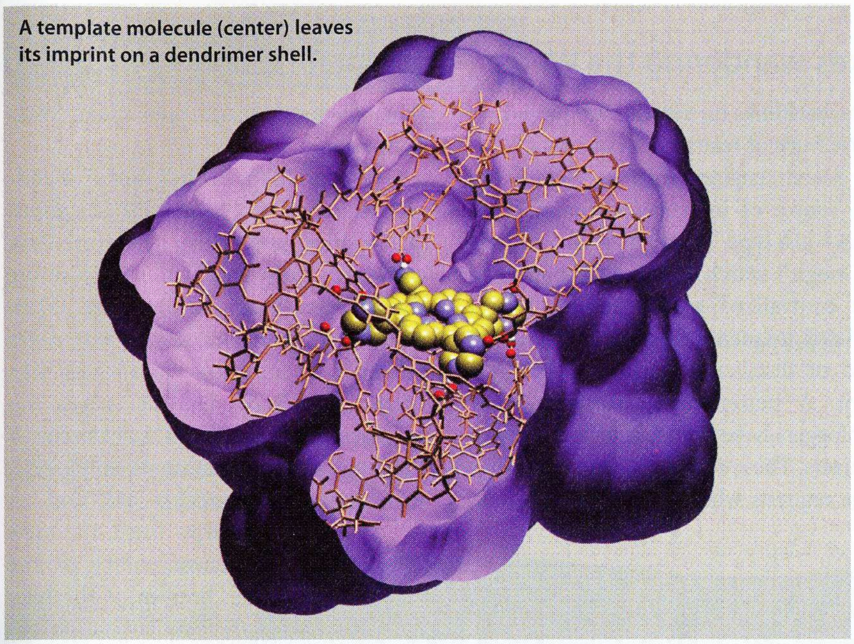
In studies in Europe, where the device was recently approved for use, patients consistently achieved "reasonably good weight loss" after implantation, says surgeon Scott Shikora, associate director of the Obesity Consult Center at New England Medical Center in Boston. Shikora, who is the lead researcher in the device's U.S. clinical trials, believes it is safer than conventional surgical procedures, all of which "have the potential for very serious complications," he says.

By itself, however, the device may not be powerful enough to overcome Americans' supersized appetites. In the first human study in the United States, some patients actually gained weight after the procedure, Shikora says, adding that volunteers in the experiment had received no dietary instructions or behavioral screening with their surgeries. Transneuronix is now conducting more trials to see whether the device, combined with dietary guidelines and support groups, can help obese patients shed extra pounds. If all the research goes according to plan, Adler says, the device could be on the U.S. market within three years. —*Rebecca Zacks*



An implantable device induces "early satiety."

SLIMFILMS (STOMACH PACEMAKER); JAMES YANG (ILLUSTRATION)



A template molecule (center) leaves its imprint on a dendrimer shell.

COURTESY OF ILYA ZHAROV AND BENJAMIN GROSSER, BECKMAN INSTITUTE, UNIVERSITY OF ILLINOIS (DENDRIMER)

MOLECULAR BLOODHOUNDS

Artificial antibodies could sniff out viruses and toxins

MATERIALS | Antibodies, the body's own biosensors, recognize and bind to foreign molecules with astonishing precision. Antibodies are incorporated in many medical diagnostic tests, but researchers have long hoped for ways to make cheap and long-lasting artificial antibodies—synthetic molecules which, when added to a patient's blood sample, would detect and latch onto specific disease markers just as effectively as natural antibodies. New work on polymer structures that mimic the binding action of natural antibodies may be bringing scientists a step closer to that goal.

To build the artificial antibodies, chemists at the University of Illinois at Urbana-Champaign start with a template molecule similar in shape to the one they ultimately want to detect. To that, they attach a handful of dendrimers, highly branched polymer molecules. After chemically linking the tips of the dendrimers to create a rigid shell around the entire structure, the researchers remove the template molecule from the center by adding water, which breaks the template's temporary bonds with the dendrimers. The end result: a dendrimer shell bearing in its center a single imprint to which molecules can bind.

Such artificial antibodies can be fabricated with the same sensitivity as natural antibodies, and they can be tailored to bind to any number of molecules, even acting as detectors of chemical and biowarfare agents in the air, says chemist Steven Zimmerman, the project's lead investigator. Best of all, Zimmerman says, "The technique is really cheap, and the biosensors are reusable. You just wash them off."

"I think this is an elegant demonstration of the [polymer imprinting] technique," says James Baker, director of the Center for Biologic Nanotechnology at the University of Michigan. The real test of the technique's potential, however, will be "whether or not these dendrimers can detect a single protein in a blood sample containing perhaps 10,000 different proteins," says Baker. At that level of sensitivity, dendrimer-based artificial antibodies might find commercial applications in AIDS or hepatitis blood tests that currently use natural antibodies. Beyond diagnostic tests, says Zimmerman, could be coatings made of dye-containing dendrimers that change color in the presence of nerve toxins and other agents. And that could mean bright prospects for artificial antibodies.—*Alexandra Stikeman*

DNA DRUGS

MEDICINE | **Turning DNA into a therapeutic treatment usually means delivering the genetic material directly into cells where it can act as native DNA does, coding for needed proteins. Now researchers are using DNA in a new class of drugs that rev up the immune system, potentially helping to boost vaccines' power and even to fight cancer—all without ever entering a cell.**

The new drugs consist of short synthetic DNA segments that mimic gene sequences found only in bacteria. The segments bind to receptors on the surface of immune cells; the cells interpret the molecules as signs of a bacterial infection and respond by ramping up the body's defenses. The first use of the technology in humans is likely to be with vaccines, in order to boost the immune system's response to inoculation, says Ethan Shevach, an immunologist at the National Institute of Allergy and Infectious Diseases. In tests on animals, the DNA segments are "unbelievably good," Shevach says.

Dynavax in Emeryville, CA, has completed early human-safety trials of an immune-stimulating DNA sequence, which when combined with a standard hepatitis B vaccine, seems to help the vaccine take effect faster and with fewer injections. Because slightly different DNA sequences may preferentially trigger specific elements of the immune system, the drugs can be tailored for particular uses such as activating natural killer cells, which attack cancerous cells. Shevach believes that the DNA fragment technology "will have a greater use [with] vaccines than as a stand-alone drug," but even that would be greatly welcomed by researchers.
—Erika Jonietz

A SLICE OF THE SYNTHETIC DNA MARKET SEGMENT

COMPANY	TARGET	STAGE
Coley Pharmaceutical (Wellesley, MA)	Allergies, asthma, hepatitis B	Human trials
Dynavax (Emeryville, CA)	Allergies, cancer, hepatitis B	Human trials
Hybridon (Cambridge, MA)	Cancer	Animal research

THE WEB'S MISSING LINKS

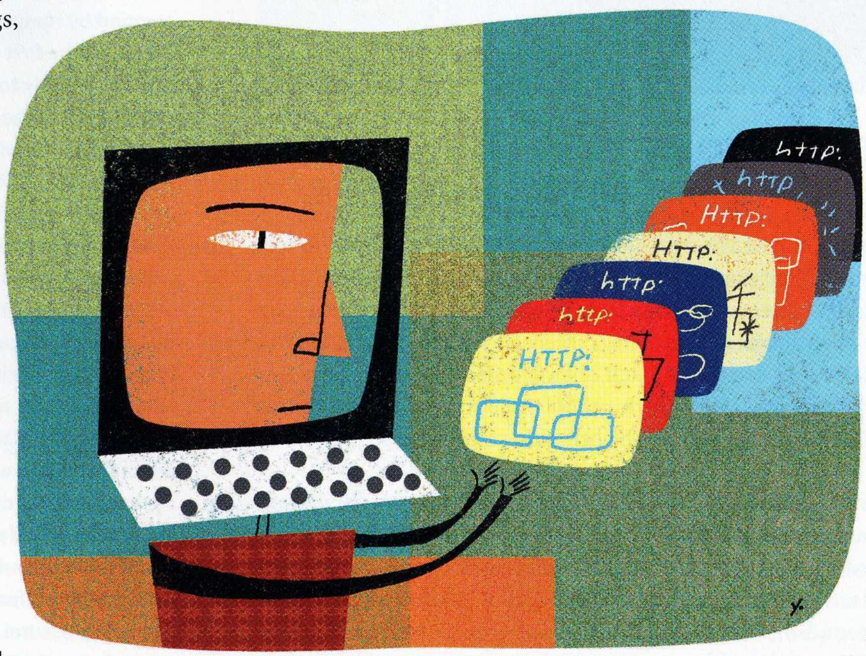
A new twist on the hyperlink makes wandering the Web twice as interesting

INTERNET | Surfing the Web, as the term implies, is all about forward motion. And like the aquatic version, Web surfing against the tide poses quite a challenge. That's because the Web hyperlink is a one-way affair: it's easy to follow links from page D to pages E, F, or G, but the Web's architecture offers no simple way to see which pages—call them A, B, and C—link to D.

Programmers have tinkered with solutions to this problem since the early days of the Web. But interest in solving it has picked up recently with the spread of weblogs, most of which are personal sites full of links and commentary. In the last two to three years, hundreds of thousands of netizens have created weblogs to chronicle their daily lives, discuss the latest news, or share expertise in their chosen fields. Many webloggers link to each other's entries, creating threads of conversation scattered across multiple sites and, consequently, a new demand for "backlinks" to see who is linking to what. "I post to my weblog; you respond in your weblog—but without backlinks, I may never know we're having a conversation," explains Mark Pilgrim, a developer and technology trainer in Apex, NC.

Webloggers, or "bloggers," say recent experiments with backlinking could benefit all kinds of online publishing. Instead of pointing readers only to sources for the item they have just read, backlinks also point to newer material that item inspired, making it easy to follow a path through the Web's marketplace of ideas. And because they can be updated automatically to reflect new incoming links, backlinks turn static Web pages into active hubs of related information.

Search engines such as Google are one source of information on inbound links—just type "link:" and a Web address in Google's search box, and a list appears. But centralized search engines aren't updated frequently enough to allow the kind of discussion tracking webloggers want. A better route, software-savvy webloggers have found, is to make use of referrers. These addresses, sent along with page requests when one clicks on a link, show where the link was found. In most cases, such referrer data are available only to the owner of the requested site, but one way to create a feedback loop is to automatically paste the addresses from server logs into the pages themselves.



That's what software developer Chris Wenham does in his Web magazine, *Disenchanted.* Wenham wrote a program that puts backlinks at the end of each article, with the most-used links listed first. Occasionally, Wenham adds his own comments or excerpts from the linking pages. "Bloggers want to be part of a community," and such backlinks give them an easy way to gather and share feedback about their ideas, Wenham says.

Ben and Mena Trott, a husband-and-wife team behind Movable Type, a popular weblog-publishing system, have enhanced their software with a more sophisticated backlinking feature. When a weblogger publishes an item that makes reference to an entry on another site, their TrackBack feature sends an announcement, or "ping," to that site. If the target site is also using the software, it will automatically add a link and an excerpt from the new commentary to the bottom of the relevant entry. The feature is intended to establish "a connection between authors" that is stronger than anything conventional referral tracking can provide, says Mena Trott.

Webloggers say academic and news sites could benefit from backlinking. "It would be nifty if the newspapers did this, so people could get a sense of the discussion going on around certain topics," says Peter Merholz, a consultant with Adaptive Path, a San Francisco interactive-design firm. An online retailer might also use the technology to offer access to consumers' reviews of its wares, suggests Wenham. But the retailer would have to be comfortable with linking to negative reviews. "You can bet that a lot of the backlinks will go to pages that have gripes," Wenham notes.

Mena Trott expects that more complex uses for backlinking features will emerge over time. "There's a lot you can do with it that we haven't figured out yet," she says.

—*David F. Gallagher*

JAMES YANG

NANO BIOMATERIALS

New combinations provide the best of both worlds

Detergent manufacturers have long used enzymes in their formulations for fighting really tough dirt. Jonathan Dordick, a chemical engineer at Rensselaer Polytechnic Institute in Troy, NY, is taking the battle against dirt a step further, using nanotechnology to design a self-cleaning plastic in which the enzyme molecules are an integral part of the material. When the plastic comes into contact with bacteria or other pathogens, the enzymes attack the microbes and destroy their ability to bind to its surface.

Dordick's innovation is far more than a boon for those challenged by a sponge and disinfectant. It reflects a growing opportunity for materials scientists to form novel combinations of biological and nonbiological molecules. Indeed, one implication of the rapidly developing field of nanotechnology is that at such small scales, the distinction between biological and nonbiological materials often blurs. As a result, researchers around the world are beginning to fabricate hybrid materials that combine nonbiological elements with biological ones such as DNA and proteins.

Such combinations could give researchers the best of both worlds. Many inorganic materials and plastics excel at conducting electricity or emitting light. Biological materials, on the other hand, are excellent at recognizing other molecules with exquisite sensitivity and can spontaneously assemble themselves into numerous complex structures. "Putting the two together will lead to some unique applications," says Dordick.

To fabricate the self-cleaning material, Dordick and his Rensselaer colleagues attach enzymes to the surface of large carbon-based molecules called nanotubes. The nanotubes, which stabilize the enzymes, are then incorporated into a polymer. The technique could work for any number of enzymes, opening the door to an array of applications, including materials that kill specific microbes or even degrade oil sludge on contact. Coatings of the enzyme-polymer material could protect implantable medical devices from scar tissue formation.

Outside the body, biological molecules can have some surprising properties. For example, Dordick has found superstrong and lightweight proteins, and he is trying to stuff them into carbon nanotubes to create "self-healing" materials. Computer simulations show that when the nanotubes break under stress, they release the proteins, which aggregate and form an adhesive. If his simulations prove correct, these hybrid materials could become components in structures such as airplane wings. As cracks propagate over time, fractured nanotubes would release the adhesive, making repairs that would prolong the wing's useful life.

Many biological molecules such as DNA can spontaneously form complex structures in a process chemists call self-assembly. Researchers are hoping to take advantage of this natural process, using it to help construct complex nanostructures. New York University chemist Nadrian Seeman, for example, is using DNA as a scaffold for assembling nanoparticles of conducting materials.

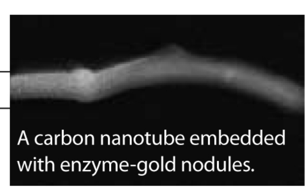
Strands of DNA with attached nanosize particles could be "coded" to assemble spontaneously into a specific structure, for instance, the configuration of a circuit. "DNA is good for doing this because the molecule is so well understood, and it's easy to control and predict what its final structure will be," says Seeman. He and his colleagues have had success making two-dimensional structures out of DNA, and they are now working on making three-dimensional crystals. One of the ultimate goals is to use DNA's knack for self-assembly as an easy and cheap way to fabricate nanoscale electronic materials or devices that could be used in ultrafast or ultrasmall computers.

Although it may be more than a decade before such bioelectronic materials are available, Dordick believes that relatively simple materials such as his self-cleaning or self-healing plastics could emerge in the next few years. "Things are moving quickly, and the number of people getting into this is increasing dramatically," says Dordick. Still, researchers readily acknowledge that they are just beginning to explore the possibilities of new hybrid materials and that eventual applications remain uncertain. "We will all go in different directions because it's such a rich field and because there are so many possibilities," predicts Seeman.

But one thing seems certain. As material scientists continue to discover novel and interesting combinations of biological and nonbiological materials, it is a field that is coming alive.

—Alexandra Stikeman

Hybrid Highlights


A carbon nanotube embedded with enzyme-gold nodules.

COURTESY OF DAE-YUN KIM

INVESTIGATOR	FOCUS
Center for Biological and Environmental Nanotechnology/Rice University	Investigating the interface of biological and nonbiological materials
Angela Belcher/MIT	Using viruses to produce nanomaterials for optical, electronic, and magnetic devices
Yet-Ming Chiang/MIT and Anand Jagota/DuPont	Identifying biological molecules to organize carbon nanotubes for new sensors and electronic devices
Jonathan Dordick/Rensselaer Polytechnic Institute	Fabricating new materials out of biological and nonbiological components
Nadrian Seeman/New York University	Using DNA to assemble inorganic particles

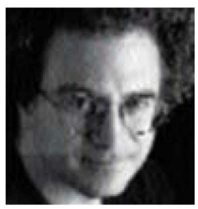

.com & go.
Booking flights at usairways.com has never been easier. Just a few clicks and you're on your way. You can also earn bonus Dividend Miles® while you do it. Plus, the most up-to-date flight information is always right at your fingertips. Which means, when you're ready to travel, there isn't a better place on the web to .com and go.
U·S AIRWAYS
usairways.com

THE RIGHTS MANAGEMENT TRAP

Faust made his deal with the devil. In return for the devil's service and knowledge, Faust agreed to surrender his body and soul after 24 years' time. By the time Faust realized the folly of his decision, it was too late. Today we are being asked to make a similar bargain—not with the devil, but with the entertainment industry. The promise is a future in which we'll download music and movies over the Internet at rock-bottom prices. It's a future where digital content—books, magazines, newspapers, and databases—will be at our fingertips. It's a future where software and information will be rented, and people will pay only for what they use. And it's a future in which computers will be inherently secure because they will be unable to run viruses and other hostile programs. It is, in short, a high tech paradise.

But it is a trap.

Every bargain has its price. In this case, the price is "digital rights management"—an industrywide project that has been under way for more than a decade and is likely to accelerate within the coming year. Digital rights management starts with a system for marking the "rights" that consumers are granted when they pay for digital media. For instance, an electronic label might say, "This music may be played on your computer but not shared with a friend." Or, "This magazine article may be viewed twice and printed once, and then it must be deleted." But the flip side of the so-called rights is another r-word: restrictions. Rights management systems will make possible software that will watch your computer and make sure you don't break the rules.



One of the great things about computers has been that you can throw away any software that comes with them and install something you like better. Digital rights management software shreds that freedom. Underneath this software is new hardware that will prevent computer users from removing the "rights management system" and installing their own systems that do not respect digital restrictions. That hardware, in turn, relies on the force of legislation. The 1998 Digital Millennium Copyright Act, in particular, makes it a crime to circumvent digital rights management software—or even to distribute information that tells other people how to do so. And proposed legislation, the Consumer Broadband and Digital Television Promotion Act, would require all computers sold in the United States to incorporate federally approved rights management technology. Similar legislation is working its way through Europe.

Essentially, consumers will be giving up their right to control their own computers. Citing the widespread piracy of software, music, and videos, the entertainment industry argues that consumers have abused that right. But managing consumers as children will have the side effect of smothering much of the innovation that made the Internet possible. Digital rights management could quash the computer revolution as we know it, transforming our machines from tools for creation and exploration into appliances that run Microsoft Office, play MP3s, browse the Web, and do little else.

Don't get me wrong. I make my living by creating and selling intellectual property, and I'm sometimes a victim of unauthorized copying. A few years ago one of my publishers started selling my books on CD-ROM. Although each disc is licensed only for personal use, at least once a month I discover that someone in Eastern Europe or Russia has taken that whole disc and put it on the Internet. Usually it's a university or a library that is engaging in such wholesale piracy.

But I would rather live with the piracy than have a computer that runs only the software that has been preapproved and digitally signed. I don't want to have my electronic movements constantly monitored and reported to some Big Brother database on the off-chance that I *might* be violating somebody's copyright.

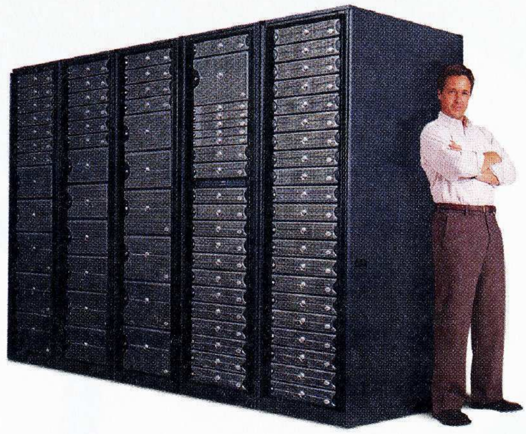
Digital rights management could quash the computer revolution as we know it, transforming our machines from tools for creation into appliances that merely run Microsoft Office and browse the Web.

This isn't the first time publishers have tried to impose unreasonable restrictions on the public. On the inside cover of one of my wife's childhood books, published in England, this ominous warning appears: "This book shall not, by way of trade or otherwise, be lent, re-sold, hired out or otherwise circulated without the publisher's prior consent." Books don't have such restrictions anymore—if they did, we would laugh at them. A hundred years ago, U.S. publishers put similar restrictions in our books; they were deemed by our courts to be unenforceable violations of "fair use." But digital rights management tools will enable publishers to turn back the clock and write the same kinds of restrictions directly into their software. Digital rights management is already at work. Incompatible coding means that DVDs sold in the United States won't play on European DVD players. This is to prevent Europeans from buying cheap DVDs in the United States.

Perhaps even more disturbing, the new protection technologies would necessarily have to block a computer from running Linux or any other open-source operating systems. Otherwise, anyone bent on unauthorized copying could create a version of Linux that didn't incorporate the copyright protection system.

The industry's antipiracy arguments are a smoke screen. Digital rights management is about strengthening monopolies, increasing revenues, and restricting our freedoms. We must not be beguiled as Faust was.

Dell | Enterprise



Dell PowerEdge™ Servers use Intel® Xeon® Processors.

Consolidate with Dell and you'll need to find a new use for your old servers.

What kind of server consolidation solutions does Dell bring to your enterprise? Just what you'd expect: A legendary focus on you, the customer, that's as relentless as our focus on driving down costs. An end-to-end solution that saves you money today and tomorrow by delivering:

- **Maximum flexibility, manageability, value and price/performance.** Our new line of PowerEdge™ servers, powered by Intel® Xeon® processors, that consistently rank at the top of industry benchmarks such as TPC.* Collectively lowering TCO and accelerating time to ROI.
- **Optimized uptime/maximized investment.** Dell's new systems management solutions deploy software, tools and services which simplify and automate server systems administration. Leveraging your IT resources and maximizing your IT dollar.
- **Server infrastructure consolidation services.** Our comprehensive portfolio includes consolidation readiness assessment, consolidation design and transformation, customer training and certification, deployment and high availability support services.
- **Flexible financing alternatives.** Dell gives you a variety of financing avenues designed to help you optimize ROI.

For nearly 20 years, we've revolutionized the way the world buys and manages technology. Now find out how Dell's direct approach can revolutionize your server consolidation. To learn more about the Dell ROI test, visit **www.dell.com/serverROI** or call us toll-free at **1-877-434-DELL**.

intel inside XEON

Flexible solutions that can cut costs today and tomorrow. Easy as DELL™

Call 1-877-434-DELL or visit www.dell.com/serverROI

*Per TPC-W 100,000 Item Count Results Test, June 2002. For more information, visit www.tpc.org. TPC and TPC-W are trademarks of the Transaction Processing Performance Council. Intel, the Intel logo and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. Dell, the Dell logo and PowerEdge are registered trademarks of the Dell Computer Corporation.


Gasoline Can, 2002
Galvanized steel, red enamel

TECHNOLOGIES THAT WOULD CURB GAS GUZZLING BY SPORT-UTILITY VEHICLES ARE WELL ADVANCED IN THE LAB. JUST DON'T BOTHER LOOKING FOR THEM AT YOUR LOCAL DEALER ANYTIME SOON. BY MARK FISCHETTI | ILLUSTRATION BY ERIC TUCKER

WHY NOT A 40-MPG SUV

To get a sense of the auto industry's progress in fuel efficiency, look no further than the 2002 Chevy Blazer. The model with automatic transmission, six cylinders, and four-wheel drive gets 18 miles per gallon (mpg), two miles less than a comparably equipped Blazer did in 1985. Indeed, in those 17 years the average fuel economy of the entire fleet of U.S. cars and light trucks declined from 26 mpg to 24 mpg—in part because of the rising proportion of gas-guzzling sport-utility vehicles (SUVs). Yet in March, when auto industry lobbyists claimed that building more fuel-efficient cars would be "too difficult," the U.S. Senate once again killed legislation that would raise the country's Corporate Average Fuel Economy standards. It was a familiar dance; Congress has not raised the standards even once during those same 17 years.

It's not that automotive technologies haven't improved; it's that the improvements have been geared toward delivering power, not efficiency. Since 1981 the auto industry has hiked horsepower 84 percent, allowing vehicles to accelerate faster even though they have gotten heavier, according to the U.S. Environmental Protection Agency. "That's what consumers want," says Fritz Indra, executive director of advanced engineering for General Motors' Powertrain division. "Each year Americans want a little more space inside, a little more power."

But is it really too difficult to build a reasonably priced SUV that can get 40 mpg and still provide the performance, comfort, and reduced emissions consumers expect? The surprising fact is that an assortment of fuel efficiency technologies exist in industry and university labs. Even more startling is that many of these technologies are based on the conventional internal-combustion engine. They don't require complex electric-gas hybrid drive trains like those under the hoods of the Toyota Prius and Honda Insight *(see Visualize, p. 83)*. Nor are they based on anything as exotic as fuel cells. If the automotive industry put some corporate horsepower behind moving these technologies into production—and that's a big if, given the lack of U.S. regulations and consumer demand—the gas-saving technologies could start hitting showrooms within five years. Indeed, if it chose to, Detroit could manufacture a 40-mpg SUV by the end of the decade.

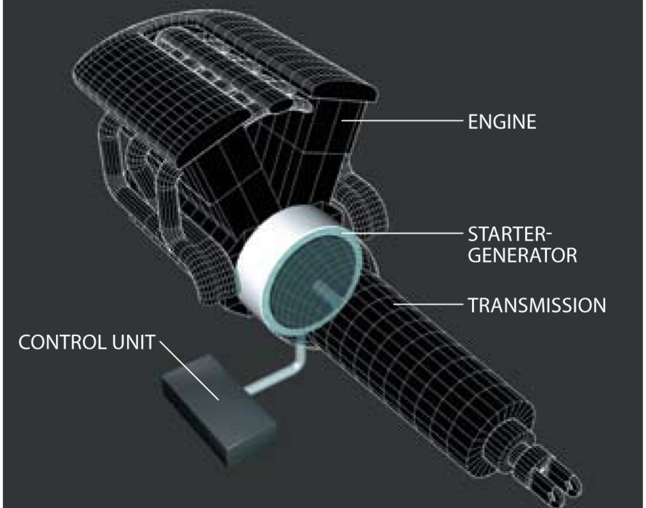
The gains would come largely from emerging technologies such as improved control systems that minimize energy losses in the engine and transmission, as well as efficient electrical components—from water pumps to engine valves—that could replace belt-driven mechanical systems. Existing technologies, such as advanced transmissions and fuel injection systems, could also play key roles if they were adopted more widely.

Indeed, if all new cars and light trucks adopted available and emerging gas-saving technologies, the average fuel economy of U.S. cars would surge to 46 mpg, up from today's 27 mpg. And SUVs could average 40 mpg, up from today's 21 mpg, according to a recent study prepared in part by John DeCicco, a senior fellow at Environmental Defense, a New York City–based environmental group. (The study was coauthored by Feng An, a modeling expert at Argonne National Laboratory, and Marc H. Ross, a physicist and automotive-policy expert at the University of Michigan.) Two-thirds of the benefit would come from improving the power train, and the rest would come from cutting weight and reducing aerodynamic drag and rolling resistance. And even though retail prices of vehicles would rise some $1,000 to $2,000, depending on the model, consumers would save that much at the gas pump within five years. "The industry doesn't lack the technology, it lacks the priority," DeCicco says.

Such improvements in gas mileage would have a huge impact on U.S. oil dependence and the environment. According to the Union of Concerned Scientists, if the U.S. fleet's fuel use improved to 40 mpg, the nation would save two million barrels of oil a day—75 percent of all the oil the United States imports from the Middle East. And it could mean a 30 percent decrease in greenhouse gases, chiefly carbon dioxide.

Automakers—while not debating the essential truth of such numbers—say that reliable, affordable versions of these new components and software controls are harder to implement than it may seem. But the manufacturers, while characteristically tight-lipped about production plans, have created advanced prototypes of these technologies and even installed early units in some vehicles. Because many of these technologies are readily available and based on the internal-combustion engine, they could have tremendous impact in the next several years. "There's a lot of potential here," says John Heywood, director of the Sloan Automotive Laboratory at MIT. "It's our best hope for continuing to reduce emissions and fuel consumption of our ever growing vehicle fleet."

AN END TO IDLING



Sandwiched between a car's engine and transmission, a powerful starter-generator could rapidly restart the engine at every traffic light and switch to generating electricity as the car moves.

FAST STARTS

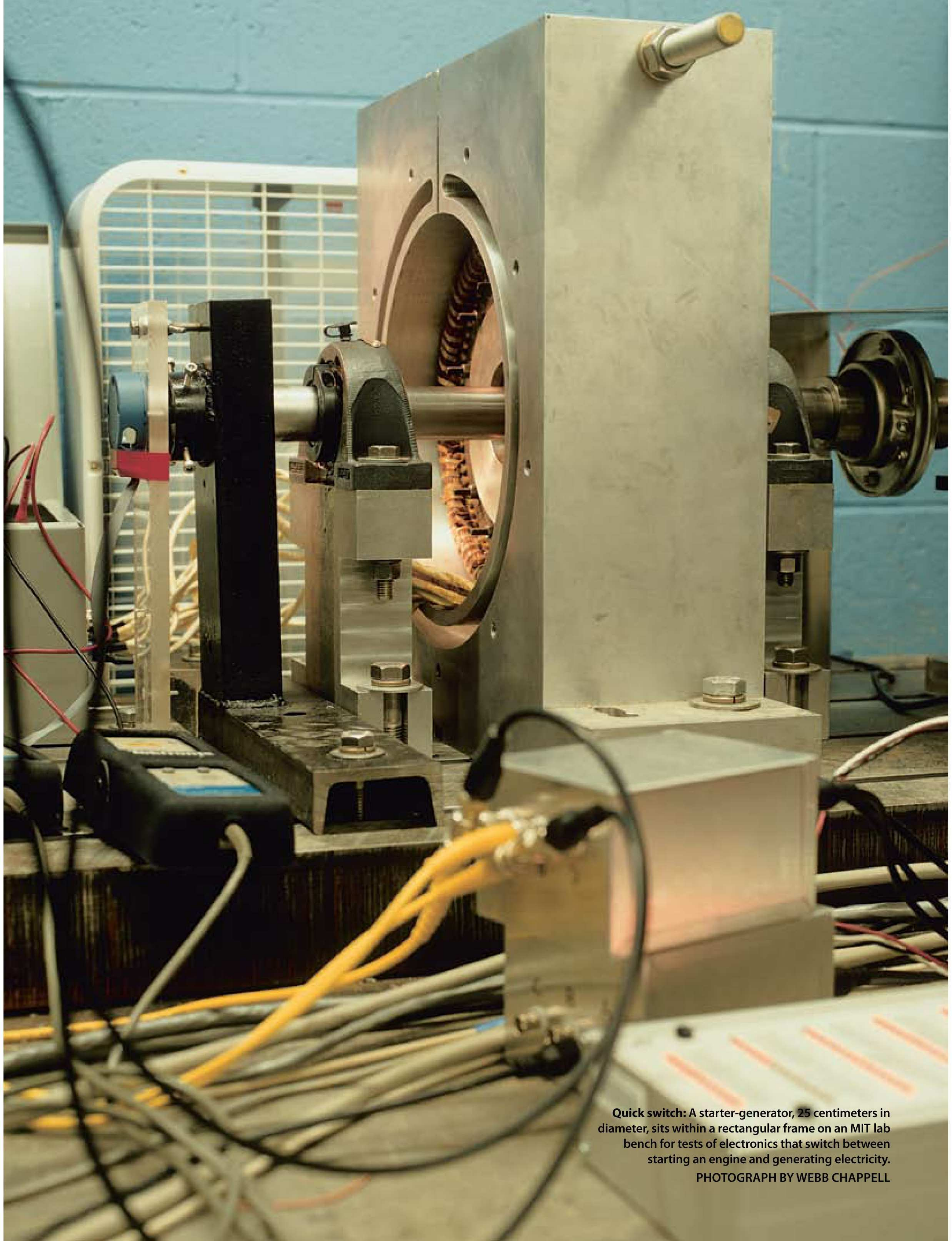
Greater fuel efficiency starts with some seemingly simple ideas, for example, shutting down the engine to eliminate wasteful idling whenever the car is not moving. But for an engine to shut down at every red traffic light, the vehicle would need a high-power device able to restart the engine immediately—far faster than a traditional starter motor—when the driver taps the gas. Sounds straightforward. But early versions were generally too slow or too noisy to keep drivers happy.

That's changing. Several auto suppliers have built prototypes of integrated starter-generators, which replace both the starter motor and the alternator, that are fast enough to crank the engine in less than half a second *(see "An End to Idling," this page)*. "The big issue is reducing cost," says Thomas Keim, an MIT electrical engineer who directs an MIT-industry consortium on advanced automotive electronics.

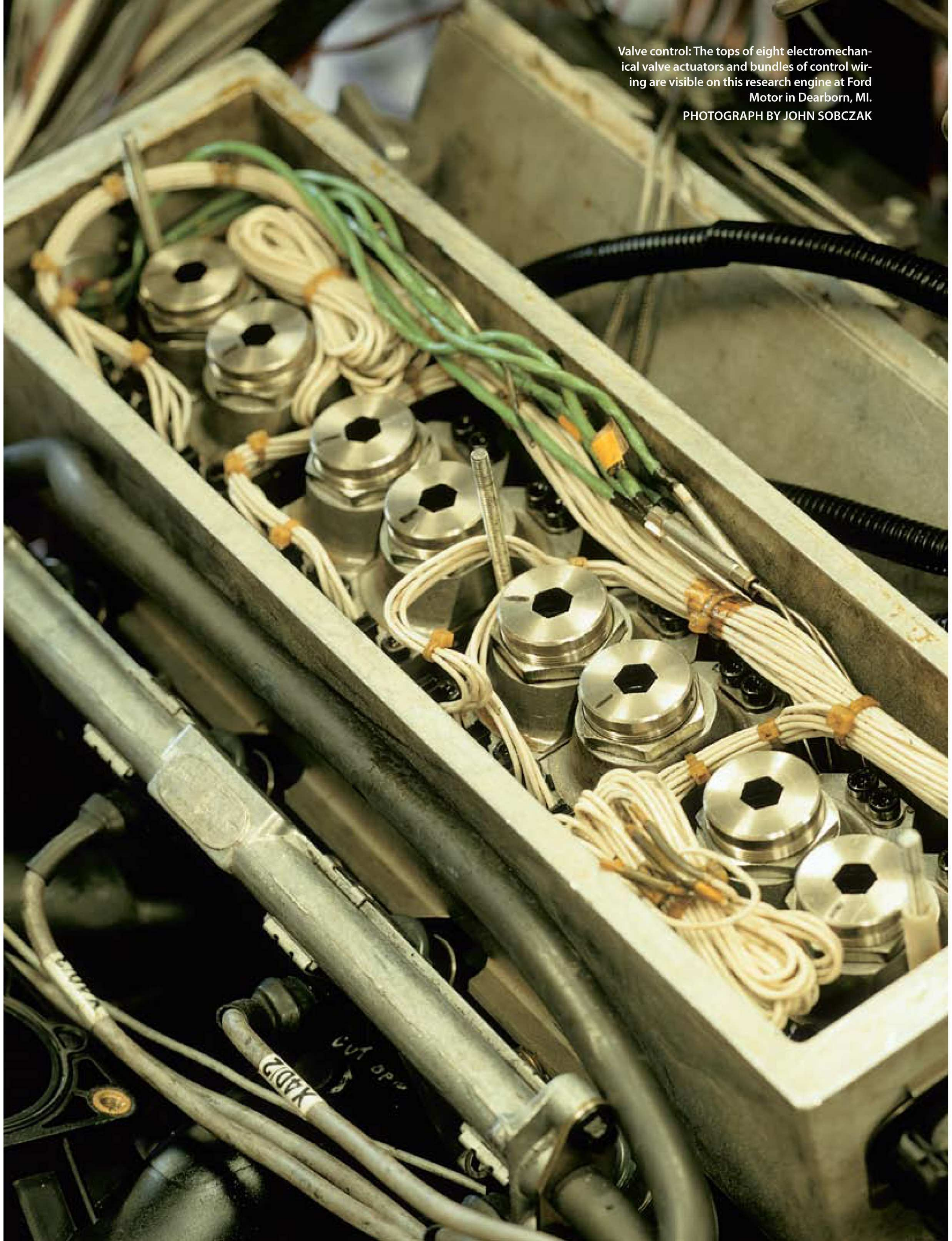
Most designs use induction motors, which must be controlled by expensive electronics that can rapidly switch between the starter-generator's dual roles of starting the engine and acting as the alternator to generate electricity. But the MIT consortium has developed a starter-generator with a simpler version of the electronics, which could reduce the cost by 20 percent. "In the automotive world, a technology that is 20 percent cheaper tends to drive the more expensive choice out of the market," Keim says. Ford has built a prototype of the consortium's design and has completed initial tests.

But there's another roadblock: the difficulty of generating

JOHN MACNEILL



Quick switch: A starter-generator, 25 centimeters in diameter, sits within a rectangular frame on an MIT lab bench for tests of electronics that switch between starting an engine and generating electricity.
PHOTOGRAPH BY WEBB CHAPPELL



Valve control: The tops of eight electromechanical valve actuators and bundles of control wiring are visible on this research engine at Ford Motor in Dearborn, MI.
PHOTOGRAPH BY JOHN SOBCZAK

enough power to keep such devices humming. Rapid cranking takes lots of power. Like most other experimental starter-generators, the MIT device, built in anticipation of a future where cars employ a higher voltage standard, operates at 42 volts. Trouble is, virtually all of today's cars still use a 12-volt system. (Exceptions include gas-electric hybrids and a 42-volt luxury Toyota sedan sold only in Japan.) Tethering a starter-generator to a 12-volt system is theoretically possible, but the starter-generator is just one of a growing number of advanced automotive electrical components on industry drawing boards. Taken together they exceed the system's limits.

Some industry experts say the voltage shift will take years: replacing an entire electrical system—which in a new car generally costs as much as the engine and transmission combined—is an expensive and complex task. But even without a complete replacement, a stopgap approach could provide a voltage boost. Manufacturers are crafting ways to install 42-volt systems beside existing 12-volt systems. The existing low-power system would remain in place, continuing to provide electricity to familiar light-duty equipment such as lights, radios, power seats, and window motors. The new high-power system would serve only heavy-duty equipment such as starter-generators and electric compressors.

The dual system "would obviously add cost," says Xingyi Xu, an engineer at Ford Research Laboratory in Dearborn, MI. Automakers would need to see considerable gains in fuel economy and consumer conveniences, he says, so "at the present time it is difficult to make that justification." Even if justifiable, such systems would take at least five years to reach market, Xu says. But because they can provide the power needed to transform the average car from a mechanical into a more efficient electromechanical machine, 42-volt systems represent an enabling technology.

SOUPED UP SOFTWARE

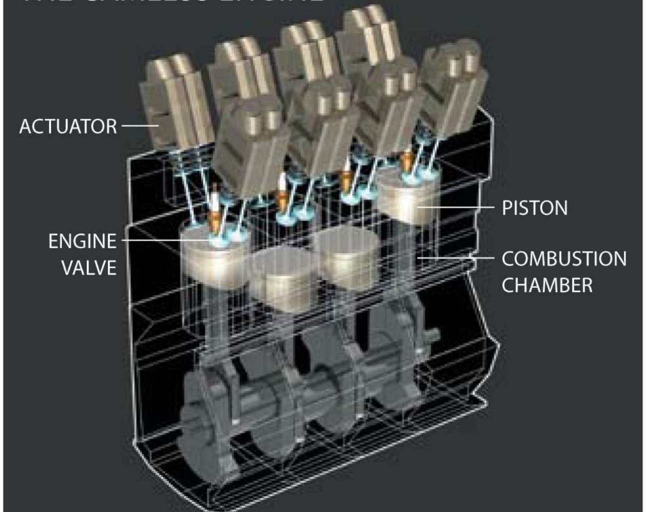
New equipment such as powerful starter-generators would raise fuel efficiency. Yet a vehicle could achieve even greater gains if the entire power train were controlled electronically.

Each component could be adjusted continuously to consume the least power necessary as driving conditions change and—equally important—could be controlled in an integrated way for systemwide savings. "Fuel efficiency would be even greater than the sum of the components," says Frank Lohrenz, an electrical engineer at Siemens VDO Automotive in Regensburg, Germany.

The savings could be significant. Integrated software-control systems could provide a 10 percent fuel-efficiency boost *(see "The Networked Car," TR September 2002)*. Siemens' software, for example, optimizes the delivery of torque—the turning force of the power train. To do this, the system electronically registers how far and how fast the driver pushes the gas pedal. Then through electronic control of such basic mechanical components as the engine, transmission, and a future starter-generator, it delivers the requested torque. The Siemens' technology takes into account 20 parameters—including vehicle speed, engine rotation speed, and transmission gear—before deciding how best to deliver torque from the combined efforts of engine throttling, transmission gear ratio, and starter-generator activation.

Engineers have traditionally considered each component as a stand-alone unit, but there is plenty of interest in integrated control because it's cheap: integrated control depends largely on software, and thus, its 10 percent fuel-efficiency boost comes at relatively low cost. "If a manufacturer sells one million cars," Lohrenz says, "the cost could be less than $5 per vehicle."

THE CAMLESS ENGINE



Electromechanical actuators atop a traditional engine provide individual control of the duration, lift, and timing of valves, which admit fuel and release exhaust from combustion chambers.

JOHN MACNEILL

DIGITAL ENGINE

The most radical advance for improving gas mileage would come about by remaking the engine itself. This means rethinking the century-old mechanics that open and close the engine valves, which let a fuel-and-air mixture into combustion chambers and release exhaust gases. For decades, a camshaft has performed this job. A spinning shaft, it moves levers that open and close valves approximately 100 times per second in a fixed pattern.

The camshaft technology works well, but it wastes fuel. The traditional configuration provides no way to change patterns in order to deliver, for example, lots of power for accelerating onto a highway and to cut back on unneeded power—saving fuel—at highway cruising speeds. In recent years, though, engineers have added mechanical equipment to the camshaft, allowing some enhanced valve control. This control includes, for example, the ability to open valves only partway when little power is needed. Honda and BMW have developed and installed such "variable valve" systems in many production cars, improving fuel economy by 5 to 10 percent.

But the ultimate move toward optimization throws the camshaft away. Instead, electromechanical actuators would provide software-driven control for each valve *(see "The Camless Engine," this page)*. By providing full control over the timing, lift, and duration of each valve motion, such a camless engine optimizes power delivery with the least possible fuel at every engine-rotation speed. The payoff is huge: a camless engine could improve fuel economy by 10 to 18 percent while also increasing engine torque by 15 to 20 percent at low speeds for faster acceleration.

The problem is that to prevent excessive wear and minimize

engine noise and vibration, valves must decelerate before landing. A camshaft, though relatively inefficient, does this quite well, thanks to its ovoid shape, which produces a corresponding acceleration and deceleration in the valve motion. Actuators are different; they slam up and down, on and off.

The way to make actuators as gentle as camshafts involves a combination of hardware and software, and many companies are working on the problem. Anna Stefanopoulou, a mechanical engineer at the University of Michigan, has already designed several promising software schemes. Within the past year Stefanopoulou's team has optimized several algorithms and is now testing ways to use feedback from the valves to achieve high-speed motion with gentle landings.

Meanwhile, to aid in this soft landing, Mohammad Haghgooie, a physicist with Ford Motor, is testing springs and pneumatic and hydraulic dampers to lessen the impact of valves without slowing them down. If successful, these improvements in electromechanical valve software and hardware could bring a camless engine to market in 2008, Haghgooie says.

With no mandate from Washington or outcry from the public, the auto industry has little motivation to change.

BRAKE FOR PROGRESS

Not all of the advanced fuel-efficiency technologies are still in the emerging stage. Even without camless engines and sophisticated software, assorted technologies for achieving better fuel efficiency are available. The list includes the "continuously variable transmission." Unlike today's automatic transmissions, which generally have four fixed gear ratios that clunk into place once engine rotation speed increases to a certain level, a continuously variable transmission delivers any of an infinite range of gear ratios on the fly. A Dutch company patented the technology decades ago; now the patents are expiring, and the transmission is already being installed in some models in the United States. The payoff can be big: in the 2002 Saturn VUE, the continuously variable transmission boosts fuel economy 7 to 11 percent, according to General Motors.

Improvements in fuel injection are also on the shelf, thanks to a recent advance known as "gasoline direct injection." By replacing the traditional indirect-injection engine with this technology, the 2002 Volkswagen Polo has improved fuel economy for city driving by 13 percent. The benefit comes from exploiting the dynamics of how fuel and air mix. In the traditional indirect injection setup, gas and air are mixed outside the cylinder and then injected. With direct injection, fuel and air begin mixing only when they are inside the cylinder, enabling the engine to use an ultralean fuel mixture during steady, low-power driving.

All in all, there is no shortage of technology available and almost ready for the auto industry to adopt. And yet, SUVs still get an average of only 21 mpg. Asked why, General Motors' Indra cites familiar industry arguments: innovations are too expensive; new components add weight, negating benefits. He says also that weight reduction—which, according to the DiCicco study, accounts for nearly one-third of the formula for boosting mileage—cuts into safety. That's the argument the industry used as part of its lobbying blitz to kill tougher fuel-efficiency legislation last March.

Roland Hwang, a vehicles expert at the National Resources Defense Council, an environmental group based in New York City, says that argument is "irresponsible." He claims the auto makers are fueling consumers' fears about safety only to persuade them to buy bigger vehicles, which, he says, yield the highest profits. He notes that federal and insurance industry tests show that the safety record of SUVs is about the same as that for other cars. Even Honda America's manager of environmental and energy analyses, John German, agrees that "if all vehicles weighed 100 pounds less, there would be no impact on safety."

The larger point is simply that with no mandate from Washington or the public, the auto industry has little motivation to change. Doug Patton, a senior vice president at Denso International America in Southfield, MI, puts the subject into perspective: "What is the customer demanding? What is the government requiring? That's how we look at it."

To researchers, this is discouraging talk. MIT's Heywood says most of these technologies have been in development for years. If the automakers wanted to, he says, they could readily make them inexpensive and reliable. "The car companies don't give their engineers enough credit for being able to solve practical problems," Heywood says. "Until management says, 'Okay, let's really go for it,' the technology doesn't get past an advanced development prototype." Giving such orders, he adds, "won't happen until management thinks it has evidence that the technology will make the product sell in the marketplace or will create a new marketplace."

Even if tough new efficiency laws are passed, others note, recent history suggests the auto industry won't accede without a fight. "Industry leaders fought catalytic converters. They fought seat belts. They said air bags would bankrupt the industry. But once the requirements are passed they find a way," Hwang notes.

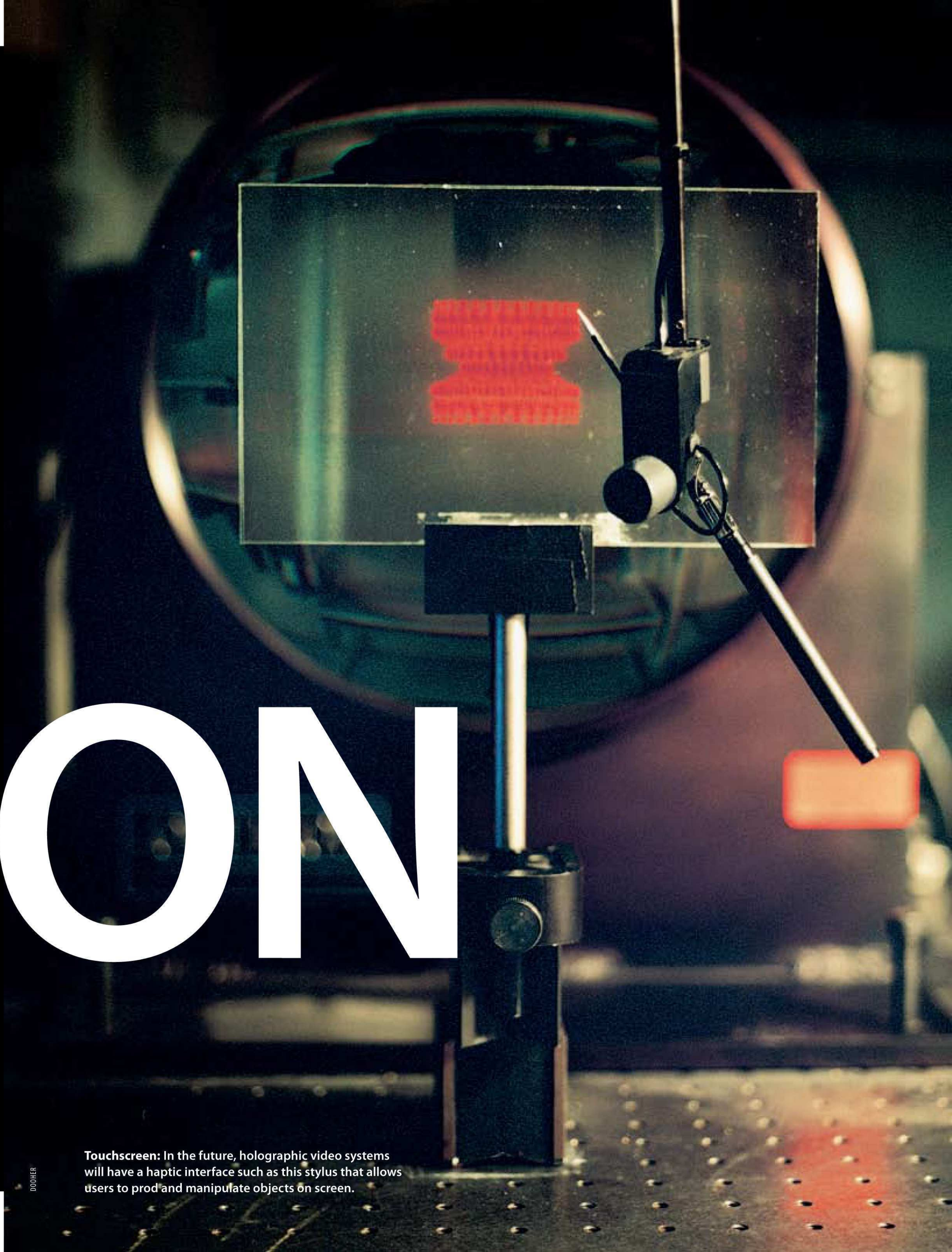
For now, the auto industry is still content to fill showrooms with perennial gas hogs. But more efficient technologies—and the software to control them—are waiting for that final push into mass production. TR

BY DAVID H. FREEDMAN

HOLOGRAMS IN MOTION

A new generation of displays will provide doctors, scientists, researchers, and product designers with unobstructed 3-D images that can be altered in real time and sculpted like clay.

PHOTOGRAPHS BY KATHLEEN DOOHER & BETH PERKINS



DOOHER

Touchscreen: In the future, holographic video systems will have a haptic interface such as this stylus that allows users to prod and manipulate objects on screen.

A half-meter-long protein floats in midair, several centimeters in front of a monitor. It looks like an oversize curled ribbon from a birthday package. As three molecular biologists maneuver around the image, studying the complex molecule from different angles, it begins to fold, slowly twisting and interlocking into a tangled knot. Its shape is a clue to the function it performs in the human body: some proteins produce chemical reactions or behave like a kind of scaffolding for cells, while others help with cell division. Creation of a drug that encourages or blocks a protein's action—say, preventing cancerous cells from dividing—could lead to more effective treatments. One of the researchers uses a stylus to prod the protein at several points. As she does so, the protein refolds itself, revealing a location that could be targeted with a drug to inhibit the protein's function.

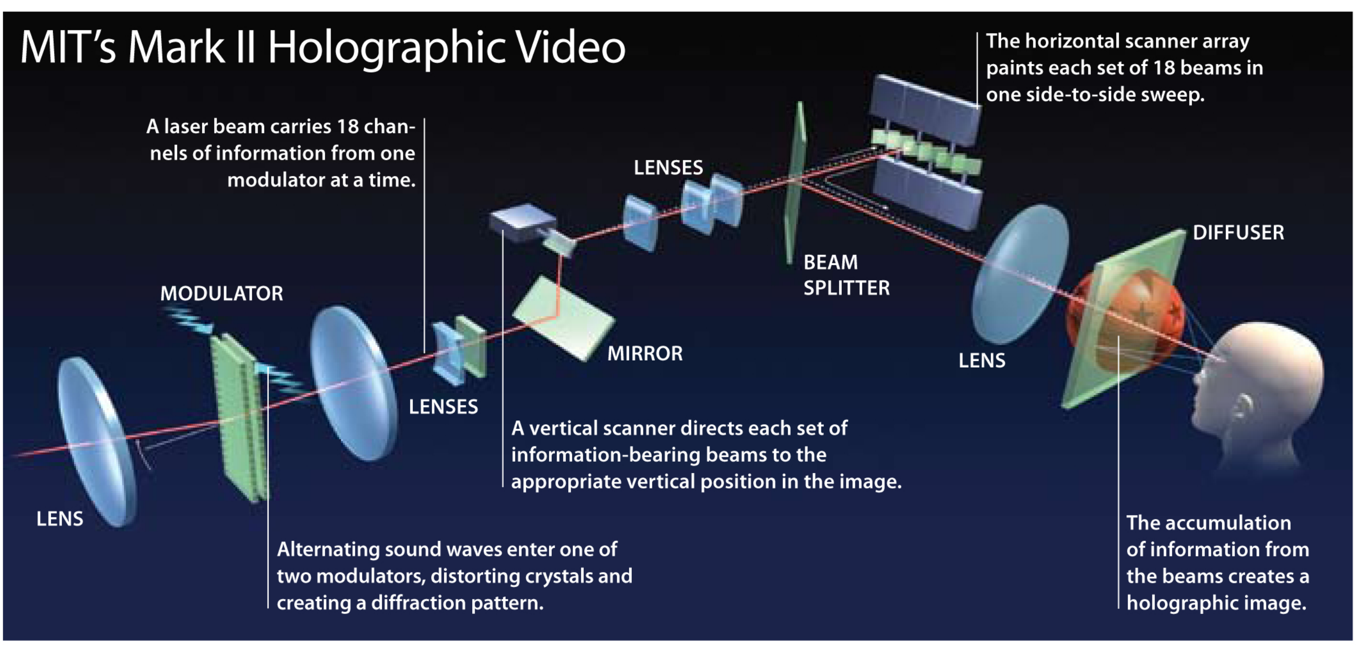
This kind of interactive science is on the way, and it will be made possible by a new generation of 3-D video displays. The technology enlists the power of holograms—or reasonable facsimiles thereof—to dish up startlingly realistic images that appear to pop out of the screen. Imagine the 3-D scenes produced by the venerable View-Master toy cranked up to "11" on the reality dial. But the new 3-D video images won't require special viewing devices. Users won't have to don the headgear or eyewear that tends to be distracting and can cause eyestrain, as they do with current so-called 3-D displays.

No. Three-dimensional holographic video images will be generated by a computer rather than being fixed in a static medium; they will be shown in full-motion color and, with input from a user, changed on the fly. What's more, viewers who move around a holographic video image will be able to see it moving from every side—a phenomenon important to realism and one that many conventional eyeglass-based systems cannot replicate.

The mainstream of doctors, scientists, researchers, and new-product developers who already rely on high-end computer displays to visualize their work will see dramatic differences in this new technology. Currently their work is constrained by the flat, two-dimensional images of conventional displays. No matter how cleverly the screens are dressed up, they can't convey all the nuances, intricacies, and immediacy of real objects in the 3-D world. Because the new video holograms produce fully 3-D images that float in space near the viewing screen, they can be examined from different angles by multiple viewers. Geophysicists examining high-resolution images of rock formations will be able to predict the location of hidden oil deposits with greater accuracy. Industrial designers will be able to modify a sports car's body using the tip of a stylus, instantly establishing the change's effect on overall design. Military commanders will be able to visualize the best battlefield scenario. Surgeons will be better able to determine the safest approach for removing a brain tumor without ever wielding a knife. "Someday we're going to wonder how we used to put up with 2-D images," says Stephen Benton, who heads the Spatial Imaging Group at the MIT Media Lab.

The group is one of two pioneering research teams leading the charge to perfect and commercialize the new generation of 3-D displays. Benton, a renowned founding member of the lab, is the inventor of the rainbow holographic images that appear on many credit cards and magazine covers. The other team, at New York University's Media Research Lab, is working on a less expensive version called 3-D autostereo display, which could become a commercial product within the next few years. The NYU effort is being led by Ken Perlin, a multimedia legend who won a Technical Achievement Award from the Academy of Motion Picture Arts and Sciences in 1996 for his development of a sound and texture technique that is widely used in films today.

The two media labs lead the quest, but they are not alone in their pursuit. In December 2000 Ford Motor and London-based QinetiQ launched Holographic Imaging, an R&D company in Royal Oak, MI, to create interactive imaging workstations for car designers. And several Japanese groups also have entered the fray, including teams at Sony, NHK Laboratories, and Nihon University. "Twelve years ago everyone thought



SLIM FILMS

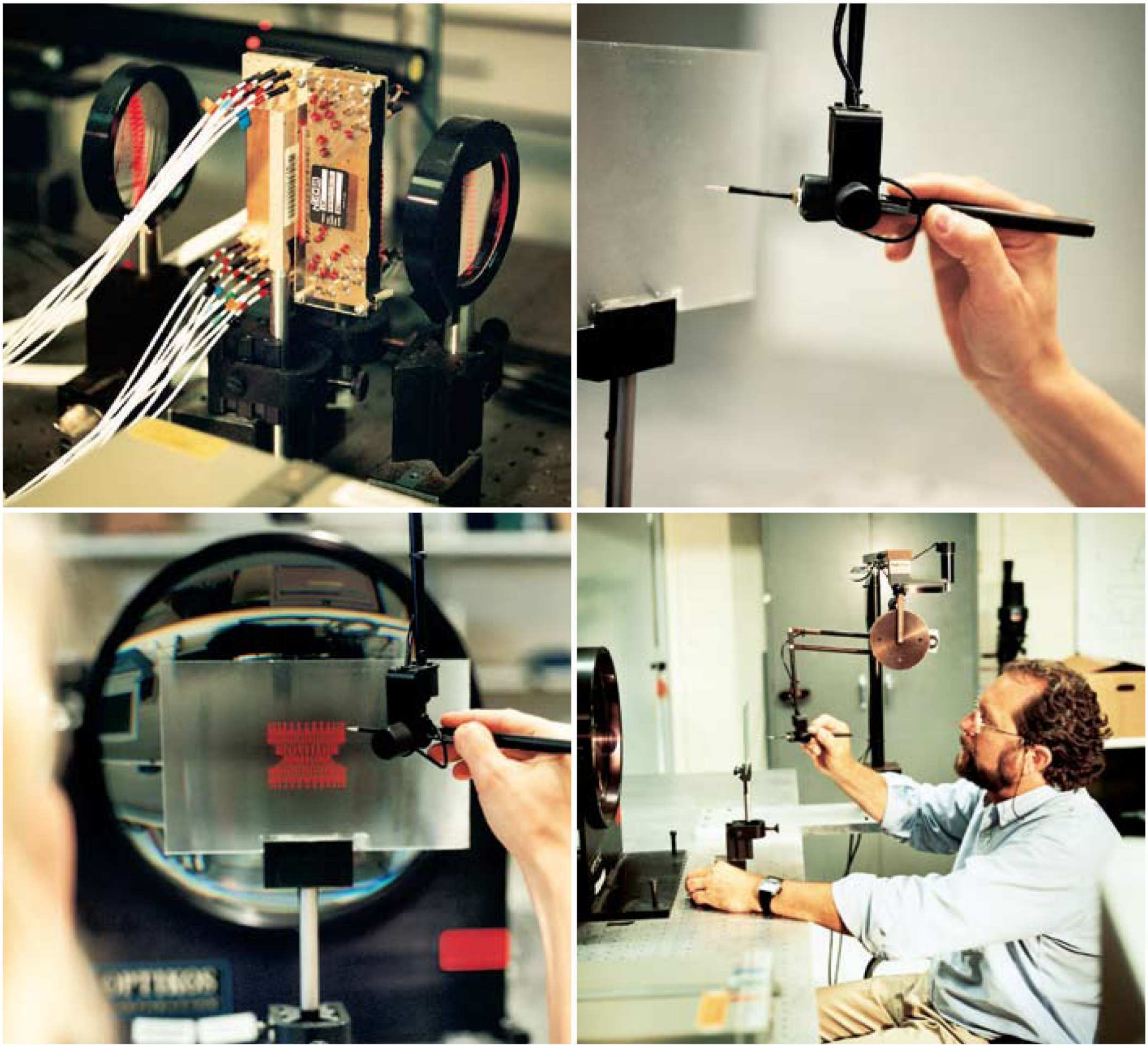


Image carving: The Spatial Imaging Group creates holograms using two crystals that distort sound waves (top left). A stylus (top right) provides force feedback, so that the lab's director, Stephen Benton (bottom right) and other researchers can "feel" the hologram as they sculpt it.

this was completely impossible," says Benton. "Now there's real competition."

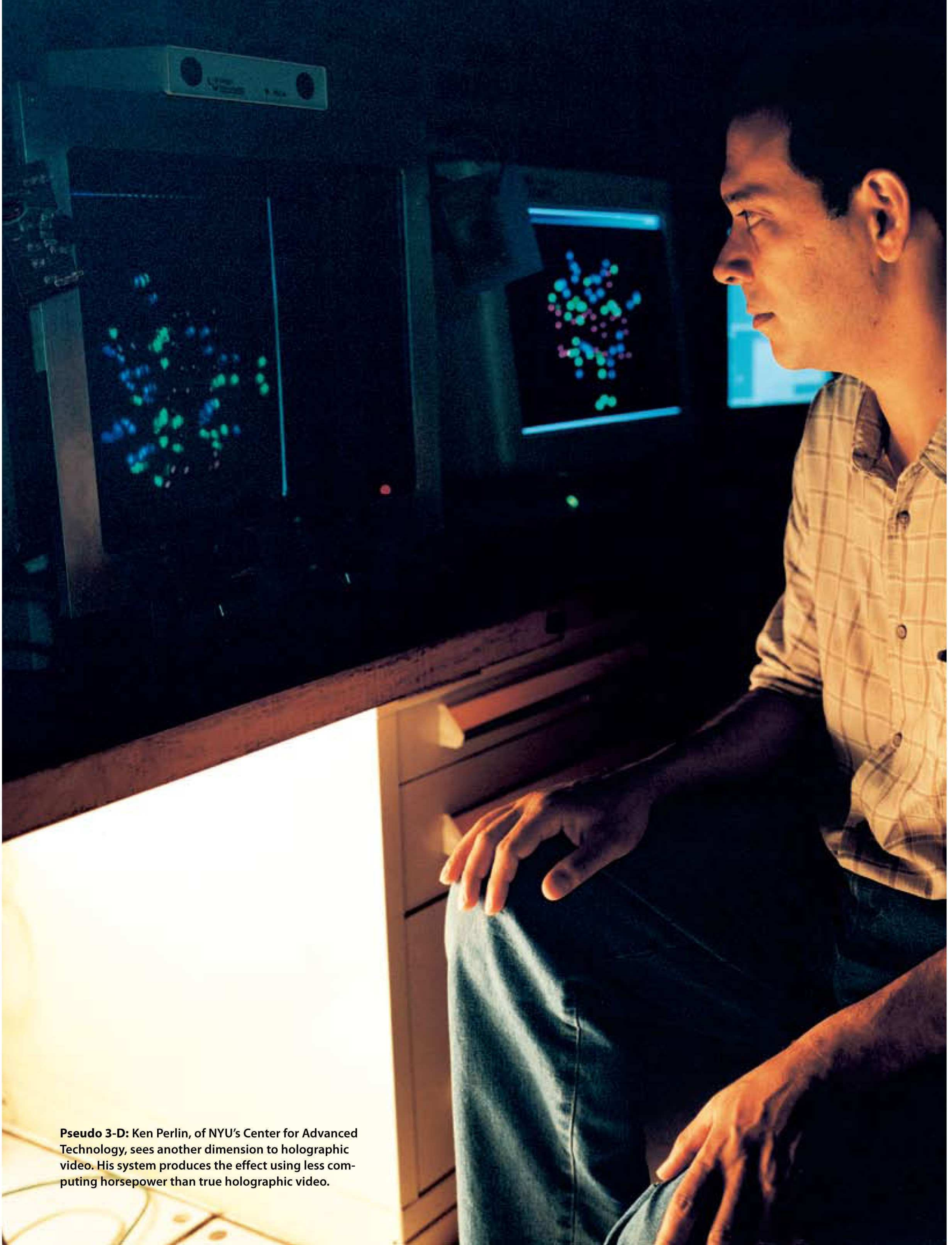
The first systems produced by these efforts will likely be specialized applications in fields such as surgical planning and automobile design. But versions cheap enough to serve as home entertainment applications should quickly follow—after all, millions of video game players would give their left control-pad thumbs to step into a fully 3-D version of Mario's world—perhaps forever rendering obsolete the two-dimensional views to which most screens have been limited. In short, sums up NYU's Ken Perlin, "All the reasons for putting up with the artifice of things being flat will go away."

CRYSTAL CLEAR HOLOGRAPHIC VIDEO

Many research teams are working to innovate holographic video, but Benton's Spatial Imaging Group at MIT has long been at the field's forefront. Here, various students and staff have been looking at the problem from every angle, so to speak, for 13 years. In recent years the main sponsors of the research have been the U. S. Navy, which believes its wartime decision-makers would benefit from looking at a 3-D representation of a battle landscape, and Honda, which hopes its car designers will be able to produce 3-D images of proposed new models rapidly. "When we first approached Honda, we were amazed to find out they had already been thinking of holography," says Benton.

The MIT effort has from the beginning focused on true holographic video, which not only holds out the promise of the highest-quality 3-D video images, but also provides the most daunting technical challenges. At its core are the basic steps of creating a standard hologram: A laser beam is split in two. One half is directed at an object—let's say, an apple. The presence of the apple distorts the pattern of light waves in the beam, modulating it. That beam is then made to intersect with its other half in light-sensitive material. When the two beams overlap, their differing patterns of light waves interfere with each other, etching a diffraction pattern of microscopic lines onto the light-sensitive material. The diffraction pattern works like a complicated lens. When a laser beam illuminates it, the

DOOHER



Pseudo 3-D: Ken Perlin, of NYU's Center for Advanced Technology, sees another dimension to holographic video. His system produces the effect using less computing horsepower than true holographic video.

microscopic lines reflect the light in a way that produces a 3-D image of the apple.

Instead of light and mirrors, Benton and his team use specially developed computer algorithms. The algorithms calculate the kinds of microscopic lines necessary for a certain hologram, convert them into sound waves, and then send the waves into a stack of tellurium-oxide crystals that have the unique property of distorting temporarily when sound waves pass through them. That distortion forms the microscopic lines of the diffraction pattern that make up a hologram. A laser beam passing through that pattern conveys the image from the crystals to a view screen (*see "MIT's Mark II Holographic Video," p. 50*).

MIT's Mark II Holographic Video Display produces surprisingly pleasing and lifelike 3-D images. In one demo, a red prototype sports car designed by Honda instantly appears to hover brightly in miniature a half-meter or so in front of the observer, all of the car's graceful lines perfectly discernible from different angles. Perhaps it's partly because of the novelty of the experience, but the mild flicker and shimmering image bars hardly distract attention from the intense realism of the effect.

Benton's group is continually making refinements in three core areas: hardware and software for the display, realism and image quality, and interactivity. Wendy Plesniak, a Media Lab researcher and consultant who as a student helped develop computing algorithms for the holographic video device, added a feature that could ultimately lead to an industrial designer's dream machine: a haptic, or force feedback, interface that makes it possible to "sculpt" the projected image with a real-life, handheld tool. As the user pokes, prods, and carves with a stylus, the holographic image changes as if it were clay on a potter's wheel, and the user senses resistance as if she were really working the clay.

Plesniak says the degree of sensation and control afforded by combining a haptic interface with holography "would provide a complete path in digital prototyping." In one demonstration, she uses the stylus to carve a red drum-shaped object as if it were rotating on a lathe; in another, a sheetlike image becomes dimpled when prodded. In general, the image produced by the system is brilliant, seems lifelike, and looks for all the world as if it is floating in space right in front of the user. "With most 3-D systems it takes a while for the 3-D effect to come in, and you never get as much depth as the math says you should," says Benton. "But you don't have those problems with holograms."

The system has some way to go, though, before it's likely to be commercialized. The biggest problem is that making a video hologram requires crunching enormous amounts of data. That may not be surprising, given that a hologram provides not just a single view of an image, but all views from any number of angles. Still the diffraction pattern from just one high-resolution hologram can easily use up more than a terabyte of data—enough to fill 1,600 compact discs. A moderately flicker-free holographic video would require at least 20 such holograms per second. Clearly, churning through 20 terabytes worth of information every second would require extraterrestrial technology: today's fastest PCs operate at one-hundred-thousandth that rate. As a result, the Mark II accepts a number of compromises in image quality in order to bring the computing requirements down to a manageable 16 megabytes per second. The system uses a single color, makes only 10.16-by-12.7-centimeter images, and generates a flickering frame-update rate of about seven images per second. In addition, because the image is stripped of the information needed to accommodate an observer's view of the top or bottom, the image changes only as the observer moves from side to side. "It's amazing how few people notice that nothing changes when you look over or under it," says Benton.

A hardware remake that is in the works should bring the system much closer to commercialization. The goals for the overhaul include switching to a parallel-microprocessor arrangement capable of churning out the high processing speeds needed to achieve larger image size, greater resolution, and a faster frame rate.

In addition, the group hopes to make the jump to an ultrahigh-resolution display screen based on microelectromechanical systems. That technology would employ thousands of tiny mirrors and laser beams—each one creating one pixel of a whole diffraction pattern. Such displays aren't expected to exist for at least a few years, but Benton notes that his group doesn't plan on seeing its work bear commercial fruit for at least another four years anyway. "Holography is hard," he says with a sigh. "That's why it's one of the longest-range projects at the Media Lab."

PSEUDOHOLOGRAPHY

Meanwhile, at NYU's Center for Advanced Technology, the other early leader in the race to produce this new wave of 3-D, Perlin's group is enlisting a nonholographic technique capable of providing dynamic, angle-adjusted images that look like those produced by holographic systems. Furthermore, the images are not conjured up by using complexly modified laser light. Instead they are displayed on

Companies Working inThree Dimensions

COMPANY	TECHNOLOGY	POSSIBLE APPLICATIONS
Actuality Systems (Burlington, MA)	Spinning screen inside a clear sphere creates 3-D images that appear to float.	Battlefield visualization, biomolecular research
Deep Video Imaging (Hamilton, New Zealand)	Two LCD screens, one in front of the other, provide a multi-dimensional effect.	Finance, navigation, petrochemical exploration, medical R&D, graphic design
Dimension 3 (Woodland Hills, CA)	Color-filtering glasses and glasses with one dark lens make moving objects stand out.	Television, print media
Dynamic Digital Depth (Santa Monica, CA)	Software recreates 3-D depth data from two-dimensional materials.	Advertising, retail, television, computer gaming
X3D Technologies (New York, NY)	LCD glasses work with an ordinary display to create a 3-D illusion.	Television, personal computers

PERKINS

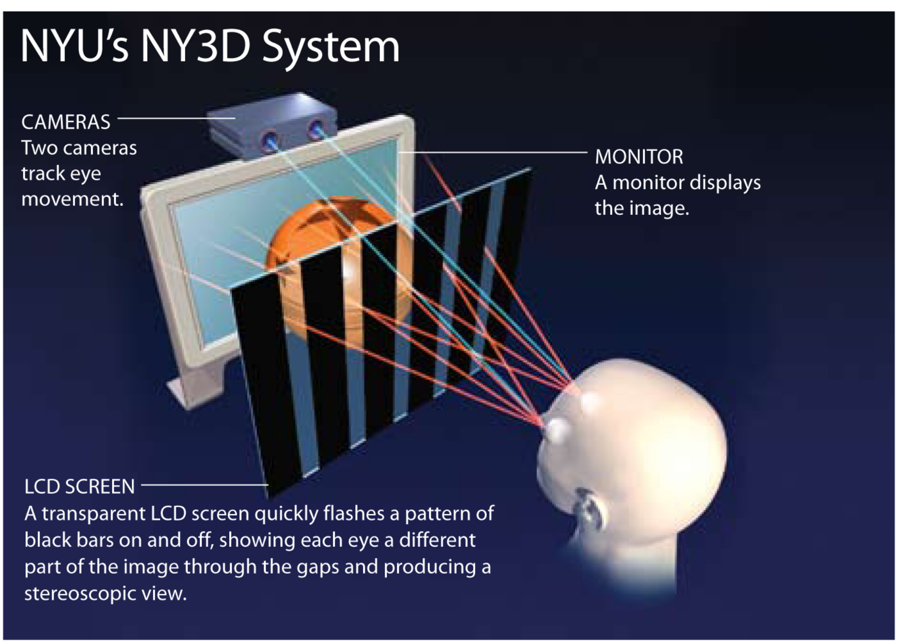
a relatively ordinary monitor in an approach Perlin calls "a holographic interface." The group pulls this off by taking advantage of the fact that most of the vast and costly processing and display horsepower needed to produce holographic video ultimately goes to waste: a hologram provides more images than those that meet the viewers' eyes; it also provides dazzling, angle-adjusted images to the many thousands of locations at which there are no eyeballs to appreciate them. Each of these distinct unperceived images have to be computed, transmitted, and displayed, because there is no practical way to limit holographic coverage to an observer's specific viewing angles. "It's like wielding an elephant gun to shoot a fly," says Perlin. His system, therefore, displays images tailored to an observer's precise position.

Though NYU's NY3D technology doesn't enlist holography, it provides an observer with much the same viewing experience as a holographic system: The mechanism is stereoscopic, providing the left and right eyes with different images, and the images change with viewing angle. And of course, no eyewear is needed.

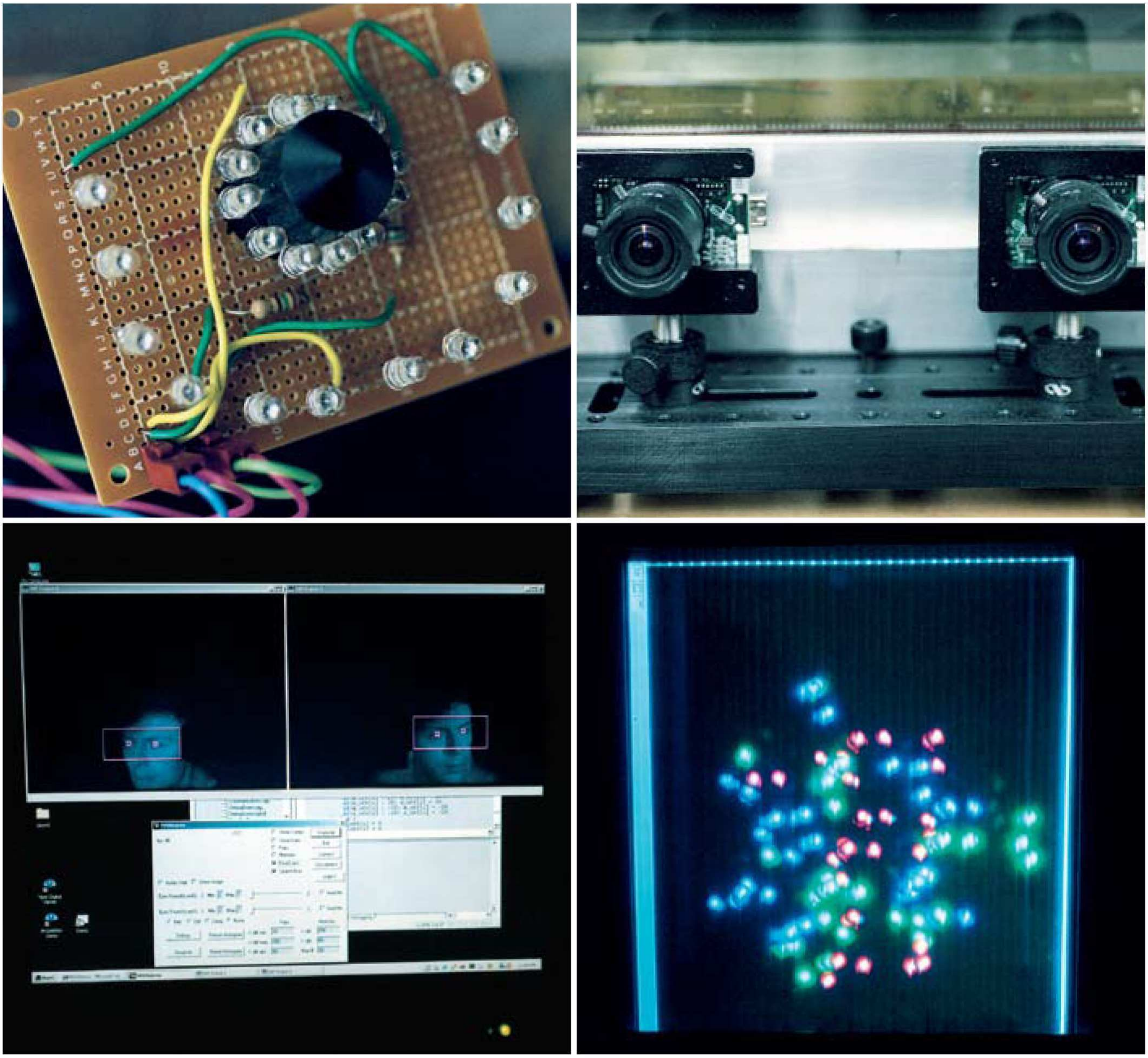
Coaxing hologram-like images from a plain screen requires two tricks. The first comes in the form of a transparent liquid-crystal display (LCD) that alters the view of the image being shown on a monitor. The display sits a half-meter in front of the monitor. On it, black stripes about three centimeters wide flash on and off, blocking vertical swaths of the image—let's say, a ball—on the monitor behind it. The effect is not obvious to the viewer, because the stripes shift 180 times per second. The speed is too fast for the viewer's brain to register the location of each stripe and at the same time, gives the monitor a chance to fill in the missing swaths for each eye. The result is that each eye sees a slightly different image through the gaps in the shutter stripes—which produce a stereoscopic sensation of depth *("NYU's NY3D System," this page)*. All this works fine—as long as the viewer's eyeballs are located exactly where the system expects them to be, each eye lining up with the appropriate image swaths on the monitor. To ensure that this is the case, Perlin's system employs a second trick, actively tracking the observer's eyes with two small cameras mounted above the monitor. Moreover, a set of infrared light-emitting diodes (LEDs) next to the cameras give the viewer an unobtrusive case of red-eye—the back-of-the-eye glow that has long been the bane of amateur photographers. The cameras can easily isolate the viewer's bright pupils, enabling them to track the eyes and adjust the location of the shifting stripes so that they always block the image in a way that sustains the stereoscopic effect.

Of course, a hologram's realism doesn't come merely from its stereoscopic properties; holographic images can be inspected from all angles as the viewer's head moves around them. By virtue of its eye-locating capabilities, the NYU system can readily track head motion and almost immediately alter the images on the monitor as needed. And indeed, a system demo that displays a rotating skeletal foot confirms not only that it provides a clear, fully 3-D image, but also that it allows one person to appraise the image from different angles—including from above or below. (The group is also working on a system that would simultaneously provide 3-D views to multiple observers, such as a team of surgeons debating the best approach to a difficult procedure or a group of video game players competing on a shared monitor.) The result is so realistic, says Joel Kollin, a researcher at the Center for Advanced Technology, that eventual purchasers of the display may want simply to hang it on the wall, where it would present images—say, a Fiji beach or a Paris boulevard—that actually change with respect to the viewer's angle. "It would be just like looking out a window," he says. As an MIT Media Lab student in the late 1980s, Kollin was largely responsible for building that group's first holographic video system.

With the recent rise of competition from groups at Sony, Ford, and other companies, such a system may well be affordable enough to allow for some elementary applications within the next few years *(see "Companies Working in Three Dimensions," p. 53)*. Because that system needs to calculate and display only the views signaled by the viewer's position at any given moment, it requires only the crunch power of an ordinary PC. The LCD screen, the eye-tracking LEDs, a high-quality monitor, and the software shouldn't add much to the total price. Perlin predicts that early-production versions aimed at specialized markets such as surgical planning will be out within three years and will be priced in the vicinity of $5,000, while the first fully holographic systems are likely to command tens of thousands of dollars. Even better, says Perlin, a few years after the first systems appear, mass-market versions of the window display will probably sell for only a few hundred dollars more than an ordinary monitor, making it a reality for the average household. Perlin, who has spun off a company to commercialize the technology, says that the venture, NY3D, already is in discussions with several large companies, including Philips and IBM, that are interested in acquiring rights to produce the display.



SLIM FILMS



Seeing stripes: The NY3D system places infrared LEDs (top left) in concentric rings around the lenses of two cameras (top right). The LEDs create red eyes (bottom left), which the camera tracks. In response, the computer adjusts the spacing of black bands on an LCD screen (bottom right).

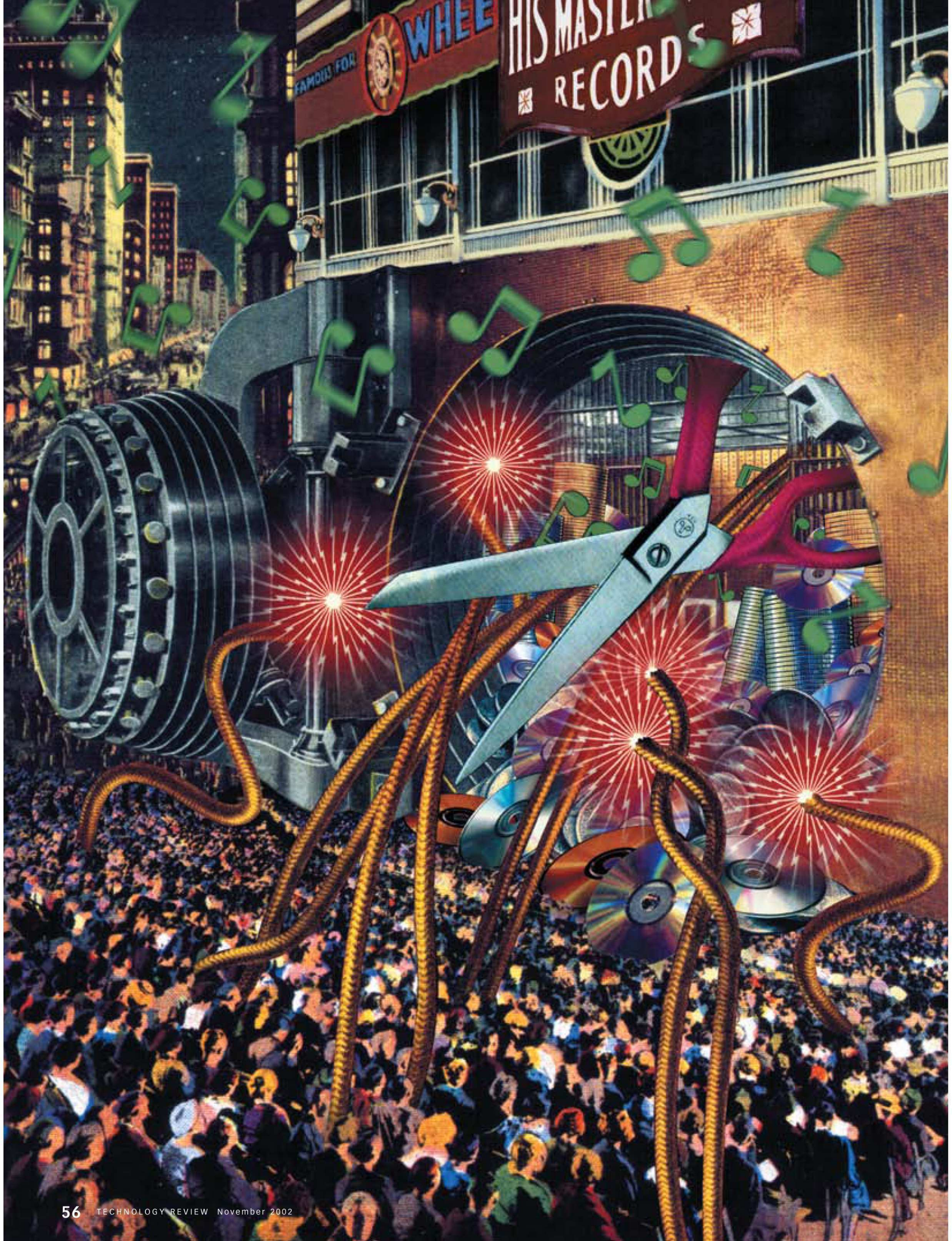
PERKINS

But while Perlin's pseudoholographic approach has a terrific cost edge and, at least for now, certain performance advantages over true holographic systems, it also has a few drawbacks. The system occasionally has trouble locking onto the viewer's glowing eyes, and rapid head movements can confuse it, causing the user to experience a temporary loss of the 3-D effect. On top of that, its image, which is subject to a number of mildly distracting artifacts, including vertical bars, wavering, and ghosting, falls a bit short of the crisp realism of a real holographic image. Much of that gap will be narrowed as the system moves from raw prototype to a commercial version, but even Perlin admits that a true holographic system would be challenging to match for image quality. "We'll certainly have commercial holographic displays, but it could take 20 or 30 years," he says.

Fear that the holographic route could take a decade or more to reach perfection explains why even the MIT Media Lab is covering its bases: it is developing a nonholographic system that works much like the one at NYU. For his part, Benton concedes it's possible that the real value of true holographic video, at least in the near future, may be in setting a "standard of realism" for pseudoholographic systems.

Until that standard is set, both teams will continue moving forward. For his part, Perlin has started researching what would widely be considered the ultimate in full-motion 3-D: a system that projects holograms into thin air—along the lines of R2-D2's projection of Princess Leia in the opening minutes of the original *Star Wars* film. Perlin believes that ultrahigh-frequency sound waves could be employed to cause air to bend light enough to form such holograms. His students have already begun proof-of-concept experiments, but he acknowledges that a working system is likely decades away and could be "ridiculously expensive."

In the meantime, there is reason to hope that pseudoholographic 3-D systems will become so cheap and effective that they could end up in many homes before the end of the decade. Then we'll all have the luxury of fretting about whether there is anything worth watching on them. "The big problem with television isn't that it's flat," Benton says. "It's that they canceled *Twin Peaks* after two seasons." TR


FAMOUS FOR
WHEE
HIS MASTE
RECORDS

MUSIC

Stung by rampant online song swapping, the recording industry wants you to buy CDs—not copy them. But its attempts to deploy antipiracy technologies are striking some sour notes with the music-buying public. BY DAVID KUSHNER

Samuel Johnson once said that "music is the only sensual pleasure without vice." Evidently, Mr. Johnson was not a punk rocker. And had there been something like Napster in the 18th century, he surely would have viewed music in a different light.

DIGITAL ENTERTAINMENT POST-NAPSTER

These days, for the estimated 40 million Americans who trade songs over the Internet, music and vice go hand in hand. After all, much of this music is copyright protected. The recording industry did successfully shut down Napster, mother of all song-swapping sites, for contributing to copyright infringement. But stifling the next generation of file-trading programs such as Kazaa, Morpheus, and LimeWire has proven more difficult. Unlike Napster, these are truly open networks that connect traders directly with each other. For the recording industry, these peer-to-peer networks are a high tech Wild West.

What's at stake? Plenty, according to a recent report by the Recording Industry Association of America, which represents the major record labels. Last year, shipments of full-length compact discs slipped by about 6 percent—the worst decline in a decade. Nearly one-quarter of the music consumers the association surveyed admitted to illegally downloading music rather than buying new CDs. The study also found that ownership of CD "burners" (disc drives that can record music onto blank CD-ROMs) has tripled since 1999; two out of five music consumers now own the machines. According to the International Federation of the Phonographic Industry, music piracy, including nearly one billion black-market CDs, cost the industry $4.3 billion last year.

Against such odds, the industry is bracing to deliver what could be a lethal counterpunch: new technologies that provide copy protection at the root of the problem, the compact disc. "We're looking for ways that will maintain the personal copying capability that consumers want," says Recording Industry Association of America president Cary Sherman, "without taking the risk of unlimited copying."

Already widespread in Europe and Asia and undergoing trial use in the United States, copy protection will transform the way consumers listen to the music they buy. The same technology could also be applied to videos and computer games. It's no surprise that the new copy-protection schemes are ruffling the feathers of some consumer advocates. These technologies "are created under the guise of preventing piracy but tend to have the effect of denying the legal right of the consumers," says Joe Kraus, cofounder of DigitalConsumer.org, which opposes copying restrictions.

In short, copy protection technology aims to put media under lock and key. It remains an open question, though, whether the locks will be strong enough to hold.

PLUGGING THE MUSIC HOLE

The show begins. Britney Spears struts onstage as the music blasts. As if on cue, thousands of teenagers hold up their glowing cell phones, so their distant friends can hear, too. In the 21st century, a live concert is only a telephone call away.

To understand copy protection technology, it's important to understand the nature of what's being protected: the music. Music is inherently free—slippery sound waves that meander through concert halls, living rooms,

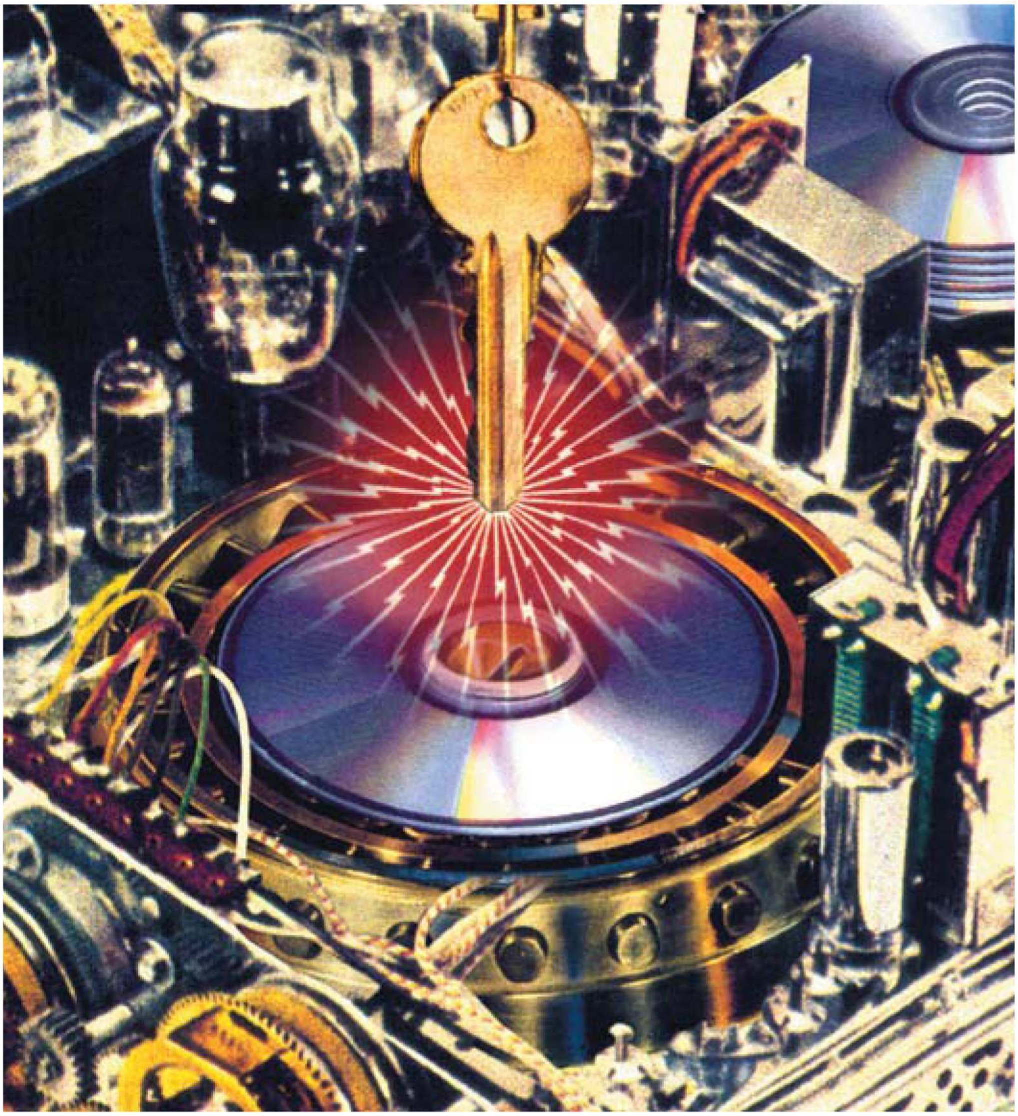
ILLUSTRATIONS BY JOHN CRAIG

and dentist offices and into listeners' ears. Selling music, in its purist form, would be like selling air. But engineers know how to restrain the unruly tunes. They carve music into vinyl. They embed it in tape. They seal it between sheets of plastic. And the record companies turn these goods into an industry. So when listeners buy Britney's latest CD, they aren't really buying the music, they're buying a wafer-thin Frisbee. The economy of content is based on physicality.

The Internet has undermined this business model, setting the music free again. Songs are being converted into digital bits, ones and zeroes that go flying over wires, spilling into homes, gushing into dorm rooms. Music fans run to the taps with buckets. And a whole industry is scrambling to stem the flow. The problem is clear. As P.J. McNealy, a senior analyst at Gartner Group, a market research company headquartered in Stamford, CT, puts it: "Music is ultimately not secure because of the way it is delivered." The mission, according to many in the recording industry, is to plug the delivery hole.

One attempted solution has been the use of technologies that allow content providers to track and control electronic media. DVD-Audio discs and digital-music subscription services, are experimenting with a technique known as digital watermarking—interleaving a file with a pattern of bits that verify authenticity without affecting the music itself. But any effort to make watermarking a common practice for protecting music CDs will, for the next several years at least, run into a big problem: many CD players are unable to read watermarks. A watermarked CD inserted into such an oblivious machine means "there's no control or protection," says Joseph Winograd, chief technology officer for Verance, a leading developer of watermarking software.

The recording industry has had similar difficulty deploying its own watermarking standards. This point was brought home painfully in September 2000 when a widely hyped coalition of music and technology companies, the Secure Digital Music Initiative, issued a public challenge to anyone who could defeat its newly minted watermark. Hackers succeeded almost immediately, and the coalition eventually fell apart, leaving an even greater need for a workable copy-protection scheme.



In the absence of a universal watermark-reading standard, the federal government has taken up the cause. Fritz Hollings (D-South Carolina), chairman of the Senate Committee on Commerce, Science, and Transportation, introduced the controversial Consumer Broadband and Digital Television Promotion Act. This legislation would require CD players and other digital-media devices to incorporate a government-sanctioned copy-protection standard if the private sector does not deliver its own standard within one year of the law's enactment.

While a standard remains elusive, technology and recording companies are heading down a more accessible and somewhat militant path. They are developing technology that attempts to nip bootlegging in the bud by clamping down on the most ubiquitous form of music distribution. If the compact discs are copy protected, then the music is no longer free.

HOW PROTECTION WORKS

For the embattled music business, copy-proof CDs are the killer app in the industry's mounting war against digital piracy. The essential idea is to manufacture discs that can be played on stereo audio machines but cannot be copied onto computer hard drives.

A few systems now on the market provide such protection. The Cactus Data Shield, developed by Tel Aviv, Israel-based Midbar Tech, is embedded in more than 30 million CDs worldwide. Try to convert a Cactus-enabled CD into an MP3 file (a process known as "ripping"), you'll get no sound at all. Sony has released 10 million CDs in Europe using its own key2audio copy-protection scheme. Such technologies are finally entering the United States as well. They debuted recently on two albums: the soundtrack *More Fast and Furious*, released by Universal Music Group, was protected by Midbar's Cactus

Data Shield. Charley Pride's *A Tribute to Jim Reeves*, from Music City Records, used the MediaCloq encryption software developed by SunnComm in Phoenix.

Each technology works by exploiting the technical differences between traditional stereos and disc players inside computers. Stereo CDs must comply with what is known as the Red Book standard, a set of technological rules defined by Philips and Sony in 1980. The rules concern, in part, how a CD separates its tracks into different sectors on the disc. CD-ROMs, on the other hand, comply with a so-called Yellow Book standard.

Red Book and Yellow Book machines read audio in different ways. Red Book devices correct for slight defects, such as skips and scratches. And herein lies the science of copyproof CDs. When a traditional CD player encounters bad code, it skips over it and keeps playing. When a CD-ROM drive in a PC runs into such data, it loops back repeatedly until it gives up and refuses to play the disc. Midbar's Cactus Data Shield modifies the way the tracks are encoded onto the disc in the Red Book format, rendering the audio invisible to a CD-ROM drive but still playable on a CD audio player.

While Cactus focuses on this high tech vanishing act, a competing technology developed by Macrovision in Santa Clara, CA, takes a different approach. Rather than strictly prohibiting copying, Macrovision's SafeAudio software just makes the results close to worthless. SafeAudio employs several different methods to achieve this effect; one is based, according to product manager Steve Phillippo, "on the introduction of errors into the music." This technique, called coding, embeds audio attributes that, when deciphered by a computer, produce a series of annoying crackles and pops. This degradation of sound quality doesn't stop people from copying a CD, but it sure makes the results unsatisfying. Another SafeAudio technique, called timing, subverts the way in which a CD-ROM player reads audio from a spinning CD; by purposefully misleading the player into reading the data either too quickly or too slowly, it contaminates the music with unpleasant sounds or simply prevents copying.

FINDING THE GOLDEN PATH

And such technologies mark just the first phase of the recording industry's larger copy-protection campaign. Consumers, as industry executives well know, want the flexibility and portability of digital-audio files. They want to listen to the new Beck recording on their living-room stereos, their computers, and their portable MP3 players. The recording companies go along with that, but they want to retain the power to control how those digital files are used. The answer: CDs that include two sets of the same songs, one set (which can be played without restriction) for the stereo, and another set (which is restricted) for the computer.

This year both Macrovision and Midbar will be rolling out products that take this dual approach. In Macrovision's scheme, the stereo tracks will continue to be protected by SafeAudio. The computer tracks, however, will be created using a technology called SafeAuthenticate, which implants an encrypted "digital signature" onto the disc. This identifying code goes further than a watermark. Not only does it verify the authenticity of the recording, it also enables a record company to set limitations on the use of the music. For instance, the code can be set to allow only a certain number of exports to a PC for playback.

Midbar's Cactus Data Shield allows listeners to play YellowBook tracks on a CD-ROM. Later this year the company will introduce a version of the software that allows listeners to copy the music to hard drives as well. But these will be curtailed freedoms; control over its use belongs to the record company, not the consumer. A song might be playable only a certain number of times, for example.

Copy protection technologies might not violate fair-use laws, but they will run up against the ingenuity of hackers. There always seems to be another way around a digital fence.

The goal of all this technology, says Eyal Shavit, Midbar's vice president for R&D, is "to find the golden path between compatibility and protection." But that's easier said than done. In 2000 Midbar tested 130,000 dual-approach CDs in Europe only to discover that because of a flaw in the Cactus scheme, 3 percent of listeners could not play the discs on their stereos. That might sound like a small percentage, but it was more than enough to sully the credibility of the emerging copy-protection wares.

More recently in Europe, some 1,000 consumers who purchased Cactus-encoded copies of Natalie Imbruglia's *White Lilies Islands* CD complained about playability problems. And in Los Angeles, two consumers filed a lawsuit against each of the major record companies (including Bertelsmann Music Group, EMI Music Publishing, Sony Music Entertainment, Universal Music Group, and Warner Music Group) after purchasing what they contend are defective products. The plaintiffs have a point: because copy-protected discs improvise on the Red Book standard, they do not technically fit the definition of a CD.

As the copy protection technologies emerge, the politicians are entering the fray. Their concern is fair use—that is, consumers' legally protected right to make copies of purchased content for their own enjoyment. Earlier this year, Representative Rick Boucher (D-Virginia) wrote a highly critical letter to Recording Industry Association of America chairman and CEO Hilary Rosen, challenging the industry's adoption of copy-protected CDs. Boucher asked what steps were being taken to inform consumers that discs were being altered, whether such technologies would detract from sound quality, and whether the software breaks any laws.

Even if the technologies do not violate fair-use laws, they face another obstacle: hacker ingenuity. CDfreaks.com, a haven for audio geeks, has posted detailed instructions for cracking Macrovision's SafeAudio. And hackers in Germany have revealed a technique that they claim disables Sony's key2audio copy-protection scheme. The very simplicity of their hack shows the magnitude of the task the recording industry faces.

Unlike copyproof systems that embed the copy protection coding right in the music bits, key2audio adds a physically distinct data track to audio CDs. When a CD-ROM reads this track, it assumes the disc is a data CD and gives up looking for music to play.

The German hackers found they could disable that protection simply by covering the data track, which resides near the outer edge of the disc, with ink from a felt-tip marker or even a piece of paper. No sooner did the news spread, than Macrovision, Midbar, and other companies posted bulletins saying that future versions of their products would be impervious to such tricks. But judging from the outcome of similar battles in the past, the hackers have the upper hand: there always seems to be another way to get around a digital fence. It is possible, for instance, to rip songs using an alternative CD-ROM software driver that allows consumers to convert a CD's songs into a file that eludes existing copy-protection schemes.

Analysts, in fact, don't believe that anything is truly immune in this digital age. "No matter how secure the music is on a CD, it can always be hacked," says the Gartner Group's McNealy. "All you have to do is put two microphones in front of your computer speakers." For someone with high-end recording equipment, the results aren't at all shabby.

Even if copy protection technology fails, the recording industry is unlikely to suffer. The player piano didn't remove the demand for musicians, nor the printing press for writers.

TRUTH IN LABELING

Despite the backlash against copy protection, momentum for the technology is building. Recording companies are using Europe as a test market for systems that will appear in the United States by the end of this year. And as politicians debate the issues of fair use, U.S. record companies will need to adopt a labeling system to notify consumers that the discs have been altered in a way that makes it impossible to copy their music onto a computer.

Such labeling is crucial not only for the recording industry, but also for the creators of portable players, says Andy Wolfe, chief technical officer of Santa Clara, CA-based SonicBlue, which makes the popular Rio digital-music players. "Consumers want to buy music and be able to listen to it on a variety of devices," he says. "It's not productive for the music industry to put out technology that creates more problems for people. If this doesn't get fixed, consumers might stop buying CDs."

With proper labeling and government approval, however, copy protection will likely be here for the long haul. Companies such as Roxio in Santa Clara, CA, a leading developer of CD-burning software, have already pledged their support. "We're going to work with whoever become leaders in copy protection," says Vito Salvaggio, Roxio's vice president of product management.

Ultimately, by employing copy protection approaches in combination with digital rights management technologies, the recording industry just might suppress the music-bootlegging vice. After all, if Eminem fans can buy a single DVD that contains digital-quality music that they can play on their stereos, their computers, and their portable MP3 devices, they'll be getting all the flexibility they need.

There's also the potential to extend the copy protection strategies developed for music to other digital media; bits, after all, are bits. This extension is especially possible given the migration from the CD to the DVD format. DVDs can hold up to 25 times as much information as CDs; to take advantage of this extra space, video and computer games, music, and video releases will come bundled with more and more additional media. If, for example, a future Tomb Raider game should come with an Angelina Jolie slide show and an Aerosmith theme song, the extra goods would need to be locked up together.

But even if copy protection technology ultimately fails, the recording industry is unlikely to suffer—at least if history is any guide. Emerging technologies have always induced panic among those ensconced in a world of traditional media. The player piano was supposed to kill the need for musicians. The printing press, writers. The television, movies. Jack Valenti, president of the Motion Picture Association of America, presented a notorious example of such panic some 20 years ago when he railed against video recording machines. In a statement to Congress, Valenti said that "the VCR is to the motion picture industry and the American public what the Boston Strangler is to the woman alone."

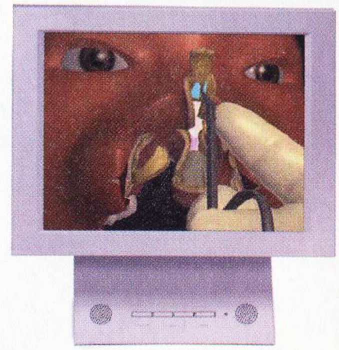
Valenti was a wee bit off in his gloomy prognostication: home video sales and rentals now bring in nearly twice as much money for the industry as do box-office sales. The fate of digital music—and the technologies being developed to control it—could well prove just as surprising. TR

Arming the Copy Cops

COMPANY	LOCATION	COPY PROTECTION ACTIVITY
Macrovision	Santa Clara, CA	SafeAudio distorts music of copied files. SafeAuthenticate puts a digital signature on a CD, restricting its use. Both are being evaluated by record companies.
Midbar Tech	Tel Aviv, Israel	Cactus Data Shield, which "hides" music on a CD to keep computers from copying it, is used on more than 30 million CDs worldwide.
Sony DADC	Salzburg, Austria	Key2audio, which disguises an audio CD as a data disc so that a computer cannot find the music, is already on 10 million CDs in Europe.
SunnComm	Phoenix, AZ	MediaCloq pioneered copy protection for CDs released in the United States.
Verance	San Diego, CA	Its digital watermarking technology, which interleaves music files with data that verify a disc's authenticity, is in use on CDs in the United States.

SOFTWARE THAT GIVES CHILDREN A SECOND CHANCE AT LIFE.

In as little as 45 minutes and for just $250, The Smile Train can give a child not just a new smile, but a new life.



Our new virtual surgery software helps produce better cleft surgeons in a fraction of the time it used to take.

We make more kinds of software for more kinds of computers than anyone else in the world.

But there's none we're more proud of than the virtual surgery software we helped develop for The Smile Train.

The Smile Train is an international charity dedicated to helping children with cleft lips and palates.

This year, The Smile Train will provide free cleft surgery for more than 25,000 desperately poor children who have no place else to turn. In as little as 45 minutes and for just $250, The Smile Train can give a child not just a new smile, but a second chance at life.

What makes The Smile Train unique is that every surgery it provides is performed by local doctors in developing countries. By using virtual surgery software, The Smile Train is able to provide free, high-quality training for doctors half a world away. This software will produce better cleft surgeons in a fraction of the time it used to take.

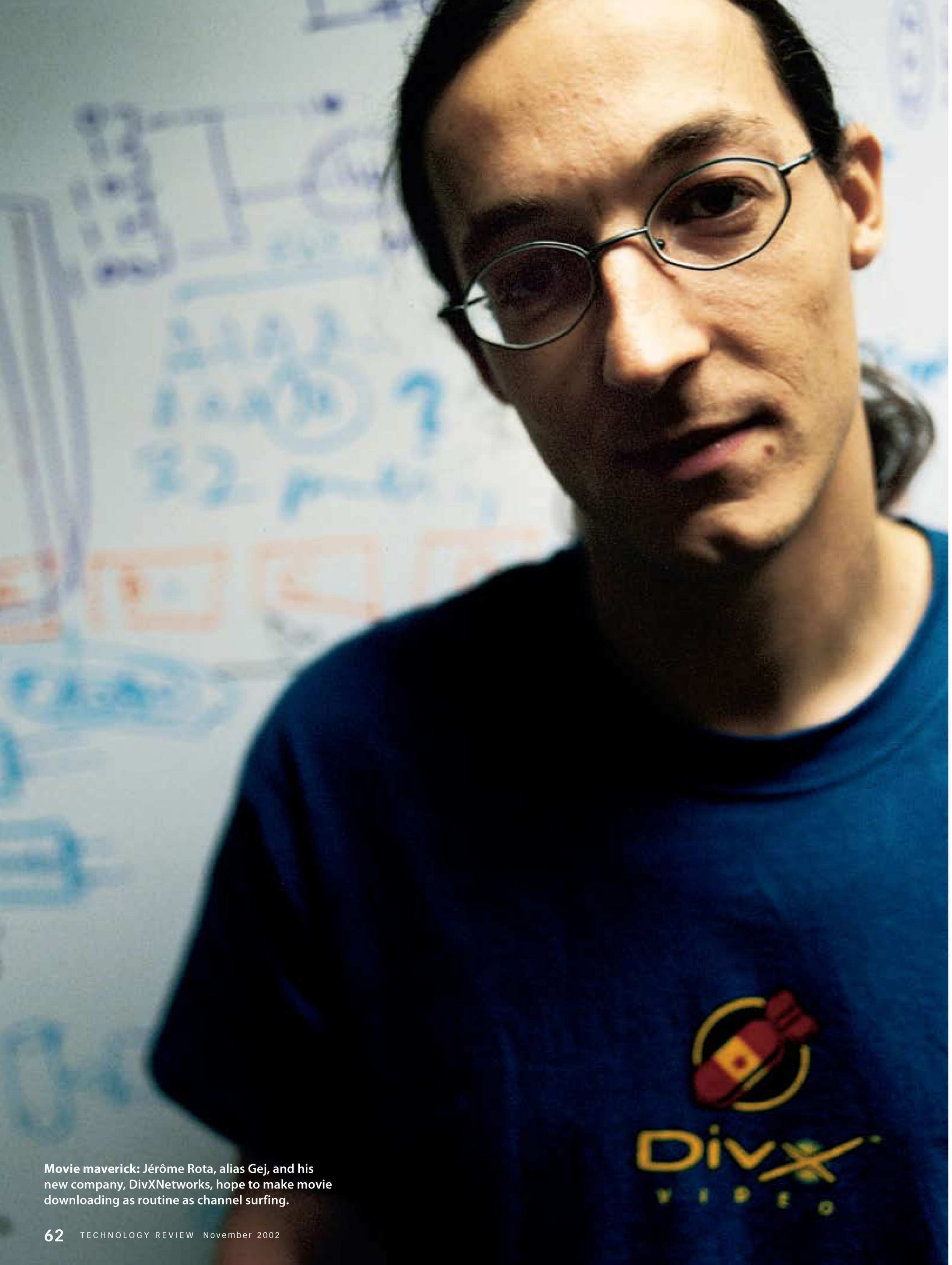
Visit www.SmileTrain.org to find out more. And if you want to help them change the world one smile at a time, make a donation, and we'll match it 100%.

We promise it will not only put a smile on the face of a child, it will put one on yours too!

TheSmileTrain
Changing The World One Smile At A Time.

To make a tax deductible donation call 1-877-KID-SMILE or visit www.SmileTrain.org.
100% of donations go towards programs, 0% to overhead or administration.
CA will match every donation dollar for dollar.

Computer Associates™



Movie maverick: Jérôme Rota, alias Gej, and his new company, DivXNetworks, hope to make movie downloading as routine as channel surfing.

MOVIES

DIGITAL ENTERTAINMENT POST-NAPSTER

The promise that movies would be delivered over the Internet is finally turning into a reality, thanks in part to a young French hacker-turned-entrepreneur. Now "Gej" wants to change how Hollywood operates. BY THOMAS A. BASS

Last summer's first two blockbuster films, *Spider-Man* and *Star Wars: Episode II—Attack of the Clones*, played on more than 3,000 movie screens and grossed more than $100 million in their opening weeks. Impressive numbers. But not as impressive as the numbers generated by these movies' actual opening nights.

A bootlegged copy of *Spider-Man* appeared on the Internet the day before the movie premiered in theaters. A copy of *Attack of the Clones*—as if to mock its title—was widely available a week before that movie's scheduled release. From that virtual opening, which was accessible to half a billion people on their home computers, its Hollywood producers grossed exactly $0.

Many bootlegged movies are "cammers," shot by digital cameras that had been sneaked into movie-screening rooms. The better copies are shot illicitly with cameras placed on tripods in the projection booth. The best ones are produced directly from studio prints or DVDs. Hopelessly dingy or surprisingly good, most of the copies have one feature in common. They are released in a format called DivX, a digital video-compression technology that shrinks movies into packages small enough to be sent over the Internet or stored on standard compact discs.

These Internet premieres mark a milestone in the long-anticipated "Napsterization" of the movie industry. Just as music file-sharing software allowed Internet users to send millions of bootlegged music files freely over the Web, DivX threatens to do the same for full-length films. "Hollywood's worst nightmare has come true," says Robert Batchelder, a research director in new media at Gartner, a consulting firm based in Stamford, CT. "You used to need a factory to make quality copies of movies. Now you just buy a computer with a CD burner."

Indeed, the analogy to Napster is apt. A computer makes no distinction between music and movie downloads, which differ only in size. A CD can hold about 650 million bytes of recorded music. A movie, which is far bigger, requires a DVD holding about 4.7 billion bytes, roughly seven times the capacity of a CD. Files that large can be sent over the Internet only if they are compressed. Compression involves chopping out redundant data and using mathematical and visual tricks that shrink an elephant to the size of a mouse.

Of the dozens of data formats for playing video on the Internet, DivX, which debuted in late 1999, was among the first and it is still considered the best for handling feature length movies. Companies such as Apple Computer, RealNetworks, and Microsoft may have pioneered commercial video formats, but for a long time they thought movies were too big and their Internet audience too small to be of interest. So, while Apple, Real, and Microsoft were concentrating on serving up small video files and streaming media, DivX, specifically tailored to films, quickly became the format of choice for compressing movies.

DivX got another jump on its competitors, which are now scrambling to catch up, with its successful launch this spring of DivX 5.0. The update gives movie aficionados a wide variety of choices for compressing their films and delivers images with near DVD quality. Sixty-five million people searched out and downloaded the new DivX software in the six months after its release. "There's no way to put the genie back in the bottle," says Batchelder.

PHOTOGRAPHS BY CHRIS MCPHERSON

JÉRÔME ROTA INVENTED—IF THAT'S NOT too grand a word for improving other people's technology—DivX in 1999. Rota, known at the time only by his Internet tag *Gej* (a Occitan word that means "crazy"), was a 27-year-old freelance video technician living in the southern French city of Montpellier. Over the summer of 1999, he had been using a beta-test version of Windows Media Player to compress and play his videos. When the official version of Media Player was released that October, however, Rota found it inferior to the earlier version. What had been a flexible tool, capable of adapting a variety of video formats, now worked only with Microsoft's proprietary software, and the files it produced were so big, he couldn't fit a movie onto a standard CD.

"I decided to set the information free," says Rota. He changed the installation instructions—a minor bit of programming—so that the new and old versions could work together. Then, by mixing and matching tools already on his desktop and by adding a few tweaks of his own, Rota created a codec—software for compressing and decompressing digital media—that married MP3 audio compression to MPEG-4 video compression. Named DivX;- (that's DivX followed by a "wink," ironic homage to a failed video system developed by Circuit City), Rota's codec was engineered to fit movies into packages small enough to be sent over the Internet, downloaded, and played on a personal computer. He set up a Web site for distributing DivX in late 1999, and in the first week alone, the program was downloaded by 50,000 people.

After he released DivX, Rota, who was still known to the world only by his nickname, began receiving messages from people who wanted to form a business with him. The most intriguing proposal came from Jordan Greenhall, a Harvard-trained lawyer who had worked for MP3.com, an Internet music site, and InterVU, a company that specialized in streaming media over the Web. After corresponding by e-mail and instant messaging, Rota, Greenhall, and a third partner, Joe Bezdek, an engineer who had been Greenhall's college roommate, incorporated themselves in March 2000 as Project Mayo. "It's not easy to make nice mayonnaise," Rota explains. "It's like video coding. It may look easy, but it's not."

Project Mayo was a virtual company. The two Americans had never met their French colleague. The idea was to stay small and secret while they perfected DivX and figured out how to commercialize it. Rota had just landed a full-time job, and he had no intention of leaving France—until a reporter from the *Wall Street Journal* tracked him down. Afraid that Rota was about to be "outed," the three partners agreed in April 2000 to meet in San Diego and go public.

The *Journal* article appeared under a headline that announced that Hollywood was facing "The 'Napsterization' of Movies." (At its peak, Napster's estimated 80 million users were downloading 100 million songs a day.) Greenhall started fielding phone calls from venture capitalists, and by summer's end he had raised $5.4 million in seed money to start a company called DivXNetworks. A second round of financing has since pushed investment close to $12 million. Because it is inadvisable to found a company using technology borrowed from Microsoft, the first thing Rota had to do was throw out his software and start all over. The company released DivX Deux, or Open DivX, in January 2001. The software was free, and this time Rota included the source code.

But Rota and his partners had ambitions beyond being another outlet for open-source software. So while continuing to give away the basic DivX codec for free, DivXNetworks began building other products it could license or sell. In March 2002, DivX 5.0 debuted at a splashy party in a Los Angeles hotel. Even the basic free version of DivX 5.0 promised to shrink movies into ever smaller packages, transmit them at faster speeds, and play them back at higher quality. Over the next two days, Rota watched in amazement—and Hollywood watched in horror—as the new software was downloaded more than a million times.

Hollywood's panic is well justified. Apart from small distributors and a few other exceptions, none of the major studios has yet to release its films online. Last year, the Motion Picture Association of America mailed 54,000 cease-and-desist letters to Internet service providers that were found to be hosting pirated movies. This year the association expects to mail more than 100,000 letters.

But, the overall trend seems inevitable. "You can't file enough law suits to shut down all these sites," says Gartner's Batchelder. "There is a huge shadow economy, a parallel universe devoted to swapping DivX movies."

DIVXNETWORKS IS PERCHED ABOVE the scrubby arroyos north of San Diego in one of the sprawling industrial haciendas that house the area's technology companies and surviving dot coms. I enter one of these low-slung buildings, which also happens to be where MP3.com got its start, and walk through a kitchen into a windowless cave the size of a basketball court. Large enough to hold most of the company's 34 employees, the room is filled with three rows of computer-laden tables. Along both sides of the tables is a phalanx of high tech Herman Miller Aeron chairs.

Rota is a tall, loose-limbed man who glides through space, peering quizzically at the world through black-framed glasses. His dark hair, pulled into a ponytail, frames his long face, and the hint of a smile tugs at the corners of his mouth. He is witty and irreverent, and he knows how strange it is for a former hacker from the media backwater of southern France to be living in California, snapping at Hollywood's heels.

In a conference room that holds two big television screens, *Bridget Jones's Diary* runs side by side in two versions. One is a store-bought DVD. The other is a compressed DivX video. At first glance, the two are nearly indistinguishable. When I open the cabinets under the televisions, I learn that the movies are playing not on video recorders but on computers. Industry wisdom says that video-on-demand will not become a mass phenomenon until someone supplies the electronic devices necessary for wiring televisions, personal digital assistants, and other consumer electronics directly to the Internet. And this is where DivXNetworks hopes to make its money. The company wants to see DivX technology built into every consumer product with a screen, allowing DivXNetworks to collect licensing fees and other payments.

This ambition pits the small startup squarely against some of the industry's giants. "I think it's going to be pretty tough," says Andrew Frank, technology officer at Viant, a media consultancy. "They're going head-to-head against Microsoft, and the best technology doesn't necessarily win."

The plan raises another question. Has Rota gone over to the "other side"?

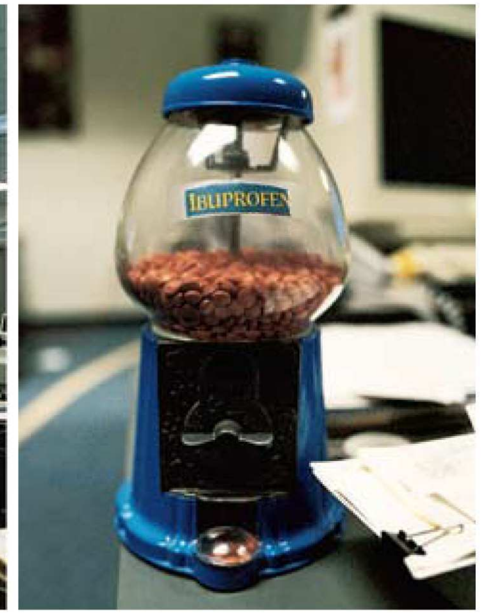
"DivX wasn't designed as a tool for pirates," Rota says. "We saw what Napster was doing to the music world and didn't want to make the same mistake. I support free speech, but I don't support the pirate's idea of 'free speech,' which is nothing more than an ideological cover for stealing other people's stuff. You can't please only the copyright holders or only the end users who want everything for free," he says. "There has to be a third way, some middle ground allowing people to get movies on their personal computers."

Later, I sit at Rota's elbow as he plays the famous beach scene from *Apocalypse Now* over and over again, each time coding and decoding the scene by a different method. He is testing improvements for the next release of his software, evaluating the pixels in every scene frame-by-frame to see how good they look, using a kitbag of psychovisual tools to get the edges crisp. "There are many tweaks involved in increasing compression. We can make you think in your mind that one image is the same as another, even when it holds a lot less information," he says.

"A DVD is a 100-to-1 compression of the original film. A DivX video is a 10-to-1 compression of a DVD. By the end, you are dealing with an image that might have a thousand times less information than the original," Rota explains. The key is to pick the information that is most important for the viewer and allocate resources accordingly. Rota's tricks include pulling bits out of the background or reducing 50 shades of black to one, using the saved memory for better results such as highlighting people's faces. "Only recently have we had the kind of computer power that allows us to put psychovisual tools into our video compressions," he says. "Video compression used to be a mathematical problem. Then it turned into a medical problem. Now I read a lot of papers by scientists on the human visual system."

It is seven o'clock in the evening, and the room is filled with the screams of players being killed in an online video game called Unreal Tournament. Outfitted with headphones and pounding furiously on their keyboards, the company's employees, their Herman Miller chairs turned into personal military-command centers, are trying not to get wasted by the fearsome firepower of their enemies. Rota is good, really good, at weaving and ducking his way out of one tight scrape after another. Armed with a sniper rifle, he shoots madly, rushing to capture the flag that is out there somewhere. TR





Dot-com artifact: The offices of DivXNetworks, where Rota and his colleagues are refining decompression methods bear striking resemblance to those prevalent during the heyday of the dot coms. An ibuprofen dispenser supplies relief to the software developers.

Make my day: Special Agent Nenette Day hunts down computer crooks from her Boston office.

ON ONE SIDE, TEEN HACKERS AND CORRUPT EMPLOYEES; ON THE OTHER, THE FBI'S COMPUTER-CRIME-FIGHTING UNITS. LET THE BATTLES BEGIN.

BY SIMSON GARFINKEL

THE FBI'S CYBER-CRIME CRACKDOWN

To protect the classified information stored on her desktop computer, Special Agent Nenette Day uses one of the most powerful tools on the planet—an air gap.

Day points to an IBM ThinkPad resting on the table behind her desk. "That computer is hooked up to the Internet," she says. "But if you break into it, have a good time: there's no secret work on it."

Two meters away on her desk sits Day's other computer—a gray-and-chrome mini-tower emblazoned with a red sticker proclaiming that its hard drive is classified SECRET. "This," she says protectively, "holds my e-mail." Day readily talks about the ThinkPad, describing how she got it as part of a big purchase by the Federal Bureau of Investigation (FBI) a few years ago and explaining that it's now somewhat out-of-date. And she happily shows off a collectible action figure—still in its display box—a colleague brought back from Belgium. It's a "cyberagent" with a gun in one hand and a laptop computer in the other. But if you let your eyes drift back to that red sticker and try to copy the bold, black words printed on it, Day will throw you out of her office.

PHOTOGRAPH BY PAUL FOLEY

Day belongs to the FBI's Boston Computer Crime Squad, one of 16 such units located throughout the United States. Each is composed of about 15 agents who investigate all manner of assaults on computers and networks—everything from lone-hacker to cyberterrorist attacks—with a dose of international espionage thrown in for good measure. Crimes range from Web site defacements and break-ins to so-called denial-of-service attacks, which prevent legitimate users from accessing targeted networks.

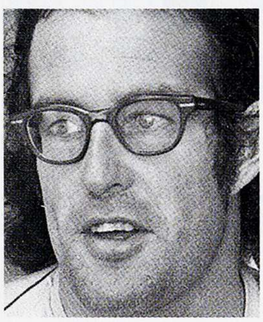
The Computer Crime Squads form the heart of the FBI's new Cyber Division. Created as part of the FBI's reorganization that followed September 11, the Cyber Division is the U.S. government's first line of defense against cybercrime and cyberterrorism. Its mission, said FBI Director Robert S. Mueller, when he appeared before the Senate Committee on the Judiciary last May, is "preventing and responding to high tech and computer crimes, which terrorists around the world are increasingly exploiting to attack America and its allies."

The emphasis on cybercrime is a big departure for the FBI. The bureau's agents traditionally got the most attention—and the biggest promotions—by pursuing bank robbers, kidnappers, and extortionists. J. Michael Gibbons worked on one of the FBI's very first computer-crime cases back in 1986; when he left the FBI in 1999, he was chief of computer investigations. "Frankly," says Gibbons, now a senior manager at KPMG Consulting in McLean, VA, "there was no great glory in the FBI on working computer investigation cases."

But that attitude is changing as Washington increasingly realizes that big damage can be inflicted on U.S. businesses through their computers and networks. Remember back in February 2000 when a massive denial-of-service attack shut down Web sites belonging to companies such as Yahoo!, eBay, and Amazon.com? It cost those companies literally millions of dollars in lost revenue. That attack, it turns out, was executed by a single high school student. Experts worry that a similar assault on the nation's electric utilities, financial sector, and news delivery infrastructure, could dramatically exacerbate the resulting confusion and possibly even the death toll of a conventional terrorist attack, if the two attacks were coordinated.

Even without the specter of terrorism, cybercrime is bleeding millions of dollars from businesses. Earlier this year,

Hall of Cyberinfamy



JOHN DRAPER, "CAPTAIN CRUNCH"

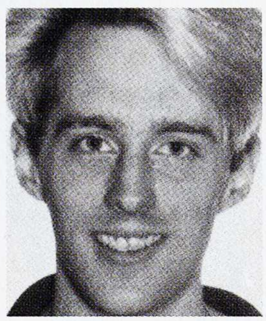
Crime: Draper discovered in 1972 that by blowing the whistle that came with Cap'n Crunch cereal, he could create the 2600-hertz tone necessary to seize control of telephone systems and place free long-distance phone calls.

Punishment: Draper was arrested in May 1972 for illegal use of telephone company property. He was put on probation, but in 1976 he was arrested again on wire fraud charges and spent four months in prison. While serving time, he started programming the Easy-Writer word processor for the Apple II computer.

KEVIN MITNICK

Crime: While in high school, Mitnick broke into computer systems operated by Digital Equipment Corp. and downloaded the source code to the operating system. By 1994 Mitnick was considered the federal government's most wanted computer hacker.

Punishment: Following a nationwide manhunt, Mitnick was arrested in February 1995 and held for four years without trial. Specific allegations were never published on the grounds of "national security." Mitnick was released from prison in January 2000 under a plea bargain.



KEVIN POULSEN

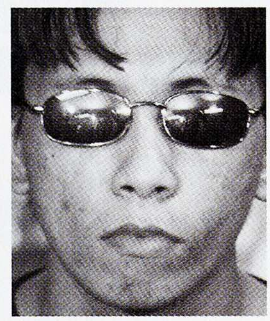
Crime: A friend of Kevin Mitnick, Poulsen rigged Los Angeles radio call-in shows to guarantee that a pal would win a car giveaway. He also broke into the FBI's National Crime Information Center, downloading active case files and alerting suspects in undercover FBI investigations.

Punishment: Poulsen spent three years in prison for hacking and was forbidden to touch a computer for three additional years after his release. He is now a journalist, covering computer security for SecurityFocus, an online business service.

"MAFIABOY"

Crime: This Canadian juvenile was responsible for the February 2000 denial-of-service attacks on CNN, Yahoo!, E*Trade, and other major Web sites.

Punishment: Arrested in April 2000 by the Royal Canadian Mounted Police working in cooperation with the FBI, the youth, whose name was withheld because of his age, pled guilty to 56 counts of computer crime in January 2001. He was sentenced in September 2001 to eight months of "open custody" and one year probation, as well as restricted access to the Internet.



ONEL DE GUZMAN

Crime: In May 2000 the ILOVEYOU computer worm spread throughout the world as an e-mail attachment. Worldwide damage in lost productivity and clogged networks was estimated at $10 billion.

Punishment: The FBI quickly traced the worm to the Philippines and identified computer science student De Guzman as the perpetrator. Phillipine authorities brought charges against him but then dismissed the case in August 2000, saying that the country's laws did not cover computer crime.

AP/WORLDWIDE PHOTOS

TR100/2003 call for nominations

What will the world look like 5, 10, 30 years down the road? Who are the leading young innovators already laying the foundation for this technological future? Help us find them and tell their stories. Nominations are now open for the 2003 edition of the TR100, *Technology Review*'s list of 100 young people whose contributions to emerging technologies will profoundly influence our world. Nominees should not turn 35 before January 1, 2003, and their work should exemplify the spirit of innovation. *Technology Review* will profile all 100 in a special October 2003 issue and recognize them at a gala dinner and awards celebration. Thank you for your nomination!

NOMINEE'S INFORMATION

*NAME ______________________ AGE ________

INSTITUTIONAL AFFILIATION(S) ______________________

____

____

*PHONE ______________________

ADDRESS ______________________

*E-MAIL ______________________

WEB SITE ______________________

What is the technical area of the nominee's work?

☐ ARTS/ENTERTAINMENT ☐ HARDWARE ☐ MEDICINE ☐ TELECOMMUNICATIONS

☐ BIOTECHNOLOGY ☐ INTERNET & WEB ☐ NANOTECHNOLOGY ☐ TRANSPORTATION

☐ ENERGY ☐ MATERIALS ☐ SOFTWARE

Please list the nominee's most important achievements.

____

____

____

Why do you think this person might be one of the top young innovators?

____

____

____

Please provide contact information for up to three other people familiar with your nominee's work.

____

____

____

NOMINATOR'S INFORMATION

*NAME ______________________

*PHONE ______________________ *E-MAIL ______________________

RELATIONSHIP TO NOMINEE ______________________

>FAX this form to 617-475-8043, attention: Alyssa Danigelis.

>MAIL this form to Alyssa Danigelis, One Main Street, 7th Floor, Cambridge MA 02142.

>VISIT www.technologyreview.com and complete this form online.

AN MIT ENTERPRISE
TECHNOLOGY REVIEW

* denotes a required field

the Computer Security Institute surveyed 503 organizations: together, they reported $456 million dollars in damages due to attacks on their computers and networks over the past year, and more than $1 billion in damage over the previous six years. Those numbers—which are the closest thing that the computer establishment has to reliable figures for the incidence of computer crime—have climbed more than 20 percent since 2001.

Day's activities show that although the FBI, the nation's premier law-enforcement agency, is starting to come to terms with cybercrime, it still has a long way to go. Agents such as Day receive special training and have access to specialized tools (many of which the FBI refuses to discuss). Their equipment, if not always at the James Bond cutting edge, is no longer embarrassingly outdated. On the other hand, the FBI's cybercrime squads are locked in a battle to keep current in the face of unrelenting technological change, and they are so short-staffed that they can investigate only a tiny fraction of the computer crimes that occur. Agents such as Day have served as only a small deterrent to hackers and high tech criminals bent on attacking a society that has become hopelessly dependent on its machines. But the deterrent is growing.

AGENTS LIKE DAY SERVE AS A GROWING DETERRENT AGAINST CRIMINAL ATTACKS ON A MACHINE-DEPENDENT SOCIETY.

How to Catch a Cybercrook

The phone rings at the FBI Crime Squad and a "complaint agent" answers. Most calls are short, not too sweet, and not terribly satisfying for the person seeking help. "We get a lot of phone calls from people who say that somebody has hacked their home computer," says Day. Others report death threats delivered in online chat rooms.

Unsettling as such events are for the victims, most callers are told that there's nothing the FBI can do for them. For one thing, federal computer-crime statutes don't even kick in unless there is at least $5,000 damage or an attack on a so-called "federal interest computer"—a broad category that includes computers owned by the federal government, as well as those involved in interstate banking, communications, or commerce. In places especially rife with computer crime, like New York City, the intervention bar is even higher.

Even cases whose damages reach the threshold often die for lack of evidence. Many victims don't call the FBI right away. Instead, they try to fix their computers themselves, erasing their hard drives and reinstalling the operating system. That's like wiping fingerprints off the handle of a murder weapon: "If you have no evidence, we can't work it," says Day. And, of course, an attack over the Internet can originate from practically anywhere—the other side of the street or the other side of the world. "We can't do a neighborhood sweep and ask, 'Did you see anybody suspicious walking around here?'" she explains.

For many computer offenses, the FBI lacks not only solid evidence but even the knowledge that an incident has occurred at all. According to this year's Computer Security Institute survey, only about one-third of computer intrusions are ever reported to law enforcement. "There is much more illegal and unauthorized activity going on in cyberspace than corporations admit to their clients, stockholders, and business partners, or report to law enforcement," says Computer Security Institute director Patrice Rapalus.

Every now and then, however, all the ingredients for a successful case come together: a caller who has suffered a significant loss, undisturbed evidence, and a perpetrator who is either known or easily findable.

Day remembers a case from October 2000. The call came from the vice president of Bricsnet US, a software company in Portsmouth, NH. Bricsnet had just suffered a massive attack over the Internet. Somebody had broken into its systems, erased customer files, modified financial records, and sent e-mail to Bricsnet's customers, announcing that the company was going out of business.

When Day arrived on the scene she went quickly for what she hoped would be the key source of evidence: the log files. These are the routine records—the digital diary—computers retain about their actions. Computers can keep highly detailed logs: an e-mail server, for example, might track the "To" and "From" addresses, as well as the date, of every message it processes. Some computers keep no log files at all. Getting lucky, Day found that Bricsnet's log file contained the time of the attack and the Internet Protocol, or IP, address, of the attacker's computer.

Every address on the Internet is assigned to either an organization or an Internet service provider. In the Bricsnet case, the address belonged to a local service provider. Day issued a subpoena to that company, asking for the name of the customer "who had connected on this IP address" when the attack took place. This information came from the service provider's own log files.

It turned out that the offending address corresponded to a dial-up connection. Each time a subscriber dials in, the service provider's log files record the date, time, username, and the originating phone number. Within a week of launching the investigation, Day had fingered a likely suspect: Patrick McKenna, a help desk worker whom Bricsnet had fired on the morning of the first attack. McKenna was arrested, charged, and convicted under the Computer Fraud and Abuse Act. He was sentenced in June 2001 to six months in federal prison, followed by a two-year parole. He was also ordered to pay restitution for the damage he had caused, which the court determined to be $13,614.11.

Masked Men and Dead Ends

Day's bust in the Bricsnet case was unusual for its speed and for the resulting conviction. That's because many crimes are perpetrated with stolen usernames and passwords. In the Bricsnet case, for instance, McKenna had broken into the company's computers using his former supervisor's username and password.

The key to cracking the Bricsnet case was caller ID and automatic number identification (ANI), two technologies

more and more Internet service providers are using to automatically record the phone numbers of people dialing up their servers. When a crime is committed over a telephone line, this information is invaluable.

"I love ANI," says Day. "The last thing you want to do is show up at Joe Smith's house because some hacker has logged in using Smith's username and password." This tool, she says, "lets you know if you are on the right track. It has made a huge difference." Not all new telecommunications technologies are so helpful, though. Many recent computer attacks, for example, flow from the growing availability of always-on high-speed Internet connections. Attackers employ computer viruses and other programs to compromise users' home computers, and then they use the compromised computers as platforms for launching other attacks without the owners' knowledge. Even worse, an attacker can jump from system to system, forging a long chain that cannot be traced. Microsoft Windows typically does not keep logs of its activity. "A lot of our investigations have been stopped cold in their tracks because someone is trotting through one of those computers," Day says, referring to cable-modem-connected PCs that run vulnerable copies of Microsoft Windows 95.

Even caller ID and automatic number-identification information can be faked by a person who has control of a corporate telephone system with a certain kind of connection to the public telephone network. So far, faked caller ID hasn't been a problem—but that could change, too.

The Internet's cloak of anonymity has made fighting crime especially tough. It's almost as if there were booths outside banks distributing free ski masks and sunglasses to everybody walking inside. "Anonymity is one of the biggest problems for the FBI crime squads," former agent Gibbons says. He maintains that cybercriminals' ability to disguise their identities does more than just complicate investigations; it also makes attackers more aggressive and more willing to take chances and do damage.

"People act differently when they don't think that they are being held accountable for their actions," says Gibbons. For years, computer security experts have maintained that corrupt employees and former insiders—such as McKenna at Bricsnet—perpetrate the lion's share of computer crime. But Day's experience contradicts this prevailing wisdom. Today things are changing: according to Day, most cases she investigates involve outsiders who commit their crimes anonymously over the Internet—frequently from overseas. Day says she has traced some 70 percent of the attacks to foreign Internet addresses. Nevertheless, insiders still represent the bulk of her investigations as they represent the most damaging attacks.

In one case, Day says, she determined that a major break-in had originated at a cybercafé in a small town in Romania. Because computer hacking is not a crime in Romania, the local police offered no assistance. Seeking help elsewhere, she phoned the café itself and talked with its owner, who spoke fluent English. "The owner said he has a bunch of cyberhackers who come there, but this is Romania, and they pay cash," Day says.

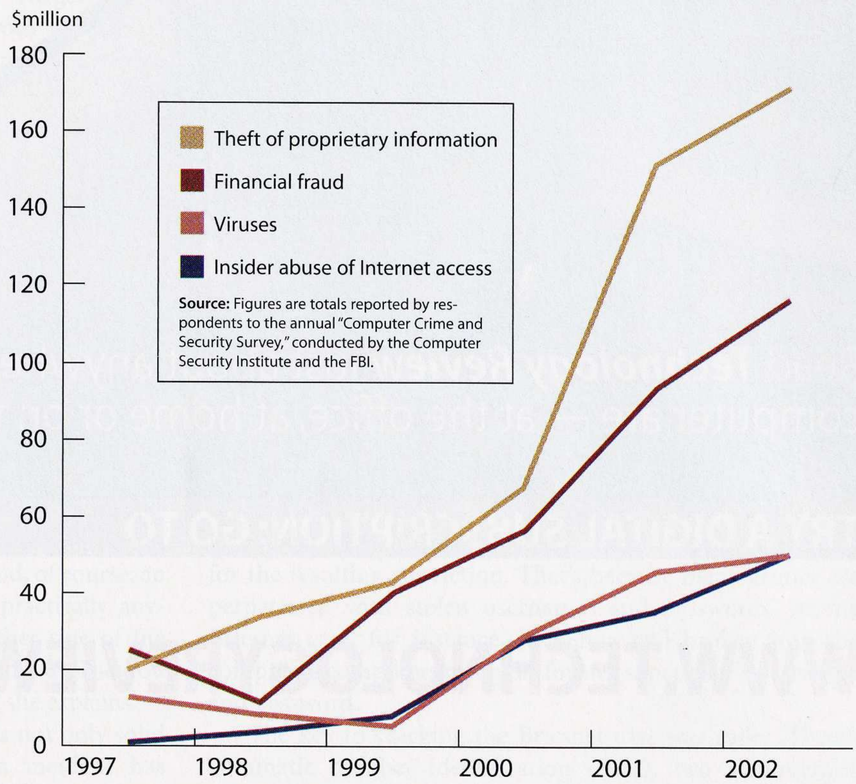
The investigation was terminated.

Attack of the Grownups

The media frequently portray the typical computer criminal as a disaffected male youth, a computer wizard who lacks social skills. In the archetypal scene, FBI agents conduct a predawn raid: with their guns drawn, they arrest a teenager while his horrified parents look on. And in fact, Day says that as recently as five years ago, juveniles made up the majority of the perpetrators she encountered. They were teenagers who broke into Web sites that had little security, and their digital crowbars were tools that they downloaded freely from the Internet. These kids made no attempt to hide their success. Instead, they set up their own servers on the penetrated computers, bragged to their friends, and left behind lots of evidence of their misdeeds.

But such attacks are no longer the most important cases that Day's office investigates. Recent years have brought "an interesting shift," she says. Now she sees attackers breaking into computers that are supposedly protected by firewalls and security systems. These perpetrators—virtually all of them adults—mount extremely sophisticated attacks. They don't brag, and they don't leave obvious tracks. "It's economic espionage," Day concludes.

The Growing Cost of Computer Crime



Source: Figures are totals reported by respondents to the annual "Computer Crime and Security Survey," conducted by the Computer Security Institute and the FBI.

It's not surprising that these cases are the hardest to crack, she says. One incident involved a suspect who had used a stolen credit card to purchase dial-up accounts at Internet service providers, specifically smaller providers that did not use caller ID or automatic number identification. He then proceeded to quietly break into thousands of computers. Day monitored the attacker for four months, trying to figure out who he was. "He was very good," she recounts. Then, in the middle of her investigation, the stolen credit card was canceled and the dial-up accounts were closed. "I was horrified," she says. The investigation fell apart, and the perpetrator is still at large.

Computer crime culprits defy stereotyping. One case that was successfully prosecuted—after a three-year investigation by the FBI—involved an assistant principal at a Long Island high school. The school administrator flooded the e-mail systems at Suffolk, James Madison, and Drexel universities with tens of thousands of messages, causing significant damage. In July 2001 the culprit, whose crimes carried punishments as high as a year in jail and $200,000 in fines, was sentenced to six months in a halfway house.

THE INTERNET'S CLOAK OF ANONYMITY MAKES ATTACKERS MORE WILLING TO TAKE CHANCES AND TO DO DAMAGE.

In the coming years the widespread adoption of wireless-networking technology will probably pose the biggest problem for the FBI cybercrime squad. These networks, based on the 802.11(b), or Wi-Fi, standard, let people use laptops and handheld computers as they move freely about their homes and offices. But unless additional protective measures are taken, wireless signals invariably leak beyond buildings' walls: simply lurking within the 100- to 300-meter range of a typical base station, an attacker can break into a network without even picking up a telephone or stepping onto the victim's property. "Many people who are moving to wireless as a cost-saving measure don't have any appreciation of the security measures they should employ," explains Special Agent Jim Hegarty, Day's supervisor.

And as the Boston cybercrime unit has discovered, wireless attacks are not just theoretical. The wireless network of one high tech company recently suffered a break-in. According to Hegarty, the attacker—an activist who was opposed to the company's product and management—literally stationed himself on a park bench outside the company's offices and over the course of several weeks, used the wireless network to "sniff" usernames and passwords of the company's president and other senior-level executives. The activist then used the information to break into the company's computers—again, making his entry through its wireless network. Armed with this illicit access, the attacker downloaded months of e-mail and posted it on the Web.

The e-mail contained confidential information about customers and their contracts. Once that became public, all hell broke loose. Some customers who discovered that they were paying higher rates than others demanded better deals; others canceled orders upon discovering that the vendor had been selling the same product to their competitors. Ultimately, the attacked company suffered more than $10 million in direct losses from the break-in. As wireless networks proliferate, attacks of this kind are likely to become more common, according to Hegarty. The advent of 802.11, he says, "is going to be a watershed event for us."

All in a Day's Work

When *Technology Review* first approached the FBI about interviewing an agent of the computer crime squad, the idea was to write about an agent's "average day." The public affairs manager at the FBI's Boston office nixed the idea: there are no average days for an FBI agent, she said. Indeed, Day says that one of the best things about her job is its endless variety.

"I might spend one day in trial preparation. I could spend an entire day milling through computer files doing evidence assessment. The next day I could be scheduled to testify in a trial. And last month I spent a couple weeks in Bangkok, Thailand, teaching police from 10 different Asian countries." She spends some days on the phone, perhaps overseeing a new case coming in from a financial institution or phoning FBI headquarters with information that needs to be relayed to other field offices. A few days later she might be off to the range for weapons training. Agent Day carries a .40-caliber Glock 23 and assists on the occasional drug raid. "It is very long work, and it's very hard," she says about her job, "but it gives you something that you would never see in the private sector."

The Glock doesn't get much use out there on the Internet, of course, but Day's FBI training in understanding criminal behavior does. She is, for example, involved in a project at the FBI's research center in Quantico, VA, developing a psychological profile of serial hackers—people who might become criminals or could be hired by a foreign government. A serial hacker could be a powerful tool for Al Qaeda or some other terrorist organization.

Moving forward, the biggest challenge, says Day, will be for society as a whole "to try to define and distinguish between what is basically online vandalism—when somebody is damaging a business or a computer—and cyberterrorism. All of those things are conflated in the discussion of the criminal prosecution of hackers. In my mind those are different kinds of contact with different social harm."

Today cybercrime is one of the FBI's top priorities—even above fraud, drugs, and gun running, says Day. But while scary talk of cyberterrorism captures the headlines, the most damaging cybercrime may actually be old-fashioned crimes being committed with new and virtually untraceable tools. Catching the new bad guys will require people like Nenette Day to stay on technology's leading edge, but it will also require an FBI able to build an organization that gives Day and her fellow agents adequate support. Furthermore, it will require the capability to bring superior computing firepower against the cyberattackers and beat them at their own high tech game.

DEMO

THE HUMAN GENOME HAS BEEN SEQUENCED ONCE. EUGENE CHAN'S TECHNOLOGY MAY MAKE IT POSSIBLE TO SEQUENCE EVERY PERSON'S GENOME, INCLUDING YOUR OWN.

PHOTOGRAPHS BY JOHN SOARES

The Human Genome Project decoded the entire genetic material of a composite person. It took more than a decade and cost $3 billion. Eugene Chan aims to sequence a genome in less than 45 minutes, for around $1,000. Chan's goal is to make it possible to sequence and store individual genomes, allowing doctors to diagnose ailments and discern which medicines will work best on the basis of a patient's specific genetic makeup. In this vision, a patient's genome sequence will be a part of a thorough medical history. To turn that into reality, Chan founded a company, U.S. Genomics, while he was in medical school. He left medical school after two years to devote himself to developing the GeneEngine, a machine he says is three to four years away from being able to quickly and cheaply sequence the human genome's roughly three billion letters. Chan and his machine are already attracting attention from leading experts. U.S. Genomics has announced a collaboration with the Wellcome Trust Sanger Institute in Cambridge, England, a major sequencing center for the Human Genome Project. And J. Craig Venter, former head of the project's rival, Celera Genomics, joined the company's board in August. Chan recently showed *Technology Review* senior associate editor, Erika Jonietz, the company's labs in Woburn, MA, and demonstrated the technology behind his sequencing machine.

THE PERSONAL GENOME SEQUENCER

Dream machine. Eugene Chan stands next to the Gene Engine, the machine he hopes will one day sequence a human genome in less than 10 minutes.

1

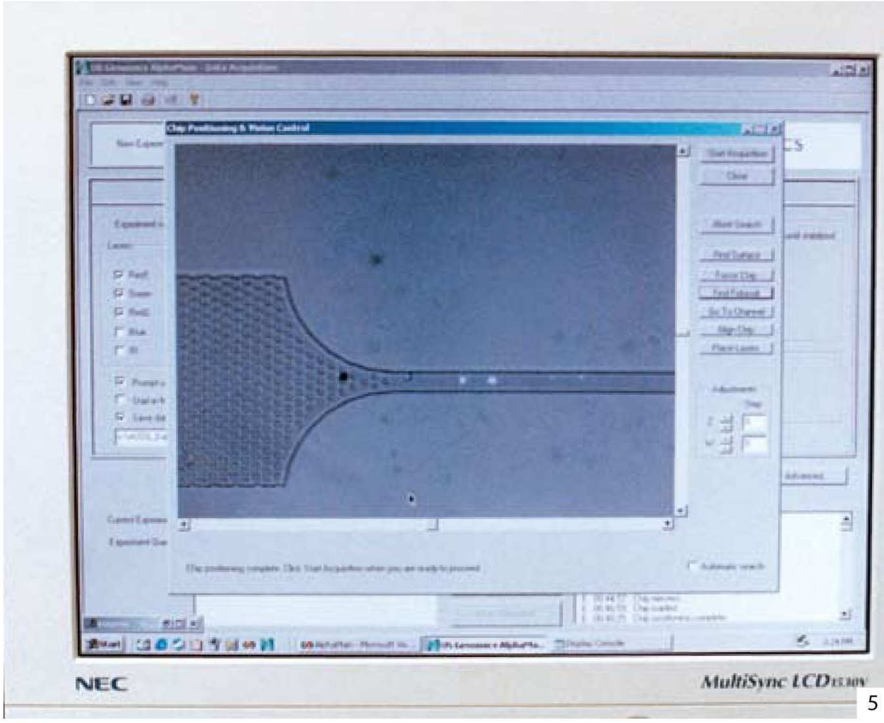
2

3

1 BEFORE THE SHOW. Chan explains that before the GeneEngine can sequence DNA, U.S. Genomics scientists must first isolate it from a blood sample and prepare it. The procedure is the longest phase of the entire sequencing process, taking one to two days, but it is still simpler than the sample preparation now widely used for sequencing. To extract the sequence information, standard methods make millions of copies of a DNA molecule, in a process that requires multiple biological and chemical steps. In contrast, U.S. Genomics's sequencing machine reads the information from a single DNA molecule, mimicking nature. "My guess is it's going to be much more accurate than conventional sequencing because there's one less step involved in terms of accessing the information," Chan says. His ultimate goal is to have the GeneEngine produce the same kind of letter-by-letter sequence data that current technologies yield. Although that's not possible yet, he says, U.S. Genomics's scientists have developed a way to read sequence information using fluorescently labeled tags that recognize and stick to specific short sequences of DNA letters, or bases. As he adds one such tag to a DNA sample in a small blue tube, Chan explains that where the tags stick to the DNA identifies sequence differences between the sample and a known reference, such as the Human Genome Project's sequence. By comparing the two, he says, researchers can decipher the sequence of the sample. Chan puts the blue tube aside, noting that the sample has to incubate for five to 30 minutes to allow the tags to stick to the DNA; then it must go through a step to remove the labels that didn't stick. The entire process may be repeated to add different tags. Once the labeling process is complete, Chan says, "you've got a DNA strand with multiple tags on it—you can think of it as a strand of Christmas lights."

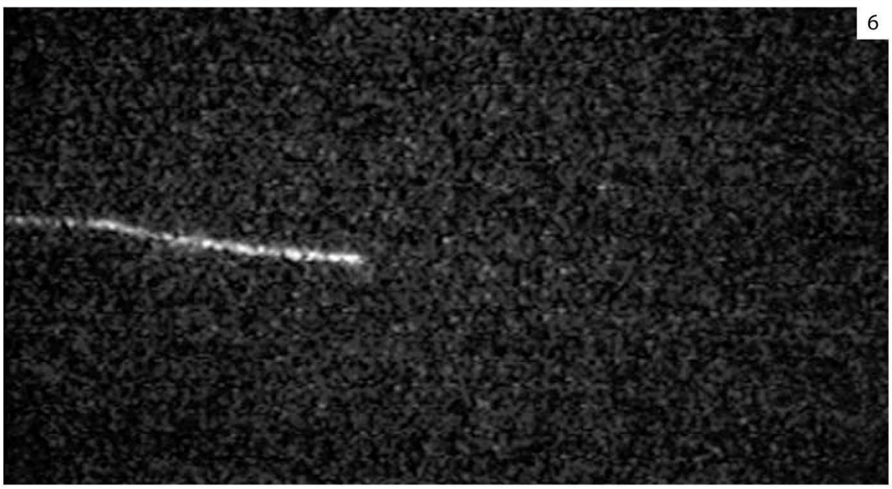
2-3 TAKING THE STAGE. The tube Chan has been working with will need several more hours of preparation, so he takes a sample that's ready to go and places a tiny amount of DNA dissolved in water—less than the volume of a tear drop—onto a small, black silicon chip. On the chip, he says, are nanoscopic channels through which the DNA will flow as the machine sequences it. The chip sits atop a glass microscope slide. "The DNA wicks in by capillary action," he says. "That's pretty much it." Chan places the slide on a stainless steel and rubber manifold for stability *(2)* and inserts it into the GeneEngine *(3)*. A quiet "pffft" of air sounds inside the machine. "When you're running the machine, the entire thing is floated on air," Chan explains, tapping the side of the GeneEngine. "Because we're trying to focus within 100 nanometers,

4



5

6



if you kind of tap, touch the ground, or anything like that, it'll vibrate." The injected air acts as a cushion. From here on, he says, everything is automated.

4 BEHIND THE SCENES. Before starting the sequencing run, Chan shows off the lasers and optics that are tucked into the back of the machine. "There are two lasers that actually sit on top of the chip and read data, very much like a DVD player," Chan says. Later, a series of mirrors and filters will focus and direct the light toward the DNA on the chip, illuminating the fluorescent tags. A photodetector will sense the light from the tags.

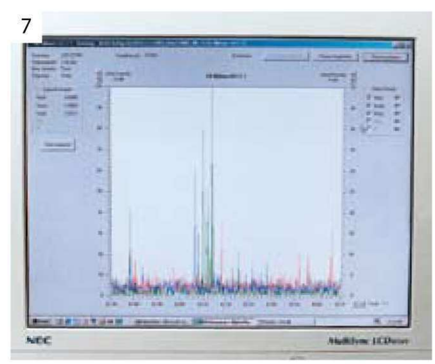
5 RAISING THE CURTAIN. Chan describes the chip on which his sequencing method relies while a camera flashes pictures of the chip onto the instrument's screen. The pictures make the chip's nanoscale features visible, showing a tapered funnel shape. Motors move the chip around to position it under the lasers. Chan points out a group of pale gray dots on the left-hand side of the screen. These are posts, he explains, each about 100 nanometers in diameter. They will stretch the DNA from its usual coiled form into a linear molecule, so the machine can read the fluorescent tags as the lasers illuminate them. "The DNA actually entangles on these particular regions of posts," Chan says. "As the molecule goes by, it snakes around those, and one end of it goes through the channel" immediately to the right. Chan describes the channel as shallow and narrow, roughly 600 nanometers across, and points out the two bright spots that are the laser beams, now focused on the chip.

6 THE STAR. Once the machine centers the channel under the lasers, fluid pressure pushes the DNA through the chip. Videotaped earlier under different lighting conditions, a single DNA molecule becomes visible as a bright streak, wending its way through the posts and unfurling into the narrow channel. The same process is now taking place inside the machine, Chan says.

7 THE NEXT ACT. As the DNA moves through the channel and past the lasers, the photodetector captures light from the fluorescent tags. Chan explains that the first laser illuminates a special label on the backbone of the DNA, allowing researchers to determine the length of the molecule being sequenced. As the DNA passes the second laser, Chan says, "the individual probe tags, which recognize variation sites on the DNA, then light up and fluoresce and give you individual probe spikes." Chan points out the green spikes in the center of the screen and says they indicate tags that have moved past the detector. Collecting data on thousands of relatively short DNA segments takes less than 10 minutes. Chan says that each such DNA molecule makes the trip past the two laser beams in a couple of milliseconds. "We capture information on these molecules as they zip by the detector at roughly 30 million bases of DNA length per second." That translates to roughly a centimeter of DNA passing through the system each second; a human genome is about two meters long.

Chan describes how, once the data from a DNA sample have been collected, U.S. Genomics software specialists must analyze it, determining differences between the sample and reference sequences in databases. Comparing the times when the DNA passes

7



by the first and second lasers allows the researchers to calculate exactly how long the molecule took to pass through the channel and helps determine the locations of the tags stuck on the DNA. "Right now, we're running 200,000 base-pair molecules through the system," Chan says. "This year we hope to get to one million. And three billion is somewhere around 2006." If plans hold, Chan's dream machine should then be able to decipher one human genome every 10 minutes. TR

COURTESY OF US GENOMICS (6)


Pick up a little something
for your chest pain.
Pick it up and dial 9-1-1 at the first warning sign of heart attack or stroke.
The faster you get help, the better your chances of survival and complete
recovery. To learn more, visit our web site at www.americanheart.org
or call us at 1-800-AHA-USA1.
American Heart
Association®
Fighting Heart Disease and Stroke
This space provided as a public service. © 1999, American Heart Association

FREEING MICKEY MOUSE

Congress has passed plenty of Mickey Mouse legislation over the years. But a few years ago, lawmakers sneaked through the actual article: a Mickey Mouse bailout bill. Now the U.S. Supreme Court can redress Congress's ill-considered public ripoff.

Formally known as the Sonny Bono Copyright Term Extension Act of 1998, the legislation addressed all "original works of authorship" (books, articles, songs, and graphic art) copyrighted since 1923, extending their copyright protection by at least 20 years. Any work copyrighted in 1978 or later retains copyright protection for the duration of the author's or artist's life and the next 70 years (up from 50 years); any copyrighted before 1978 is protected for 95 years, regardless of how it was produced or when the author or artist died.

Why, in 1998, did Congress feel the urgent need to extend copyright? The legislators certainly weren't being lobbied by the Dead Poets Society. The plain fact is that this was a corporate giveaway. The beneficiaries are big publishing conglomerates including AOL Time Warner and movie studios such as Disney. The first Mickey Mouse character, copyrighted in 1928, was set to revert to the public domain in 2003. Now thanks to Congress, Disney can keep Mickey until 2023. Considering that the cash cow mouse helps earn the company billions of dollars a year in products and theme park revenues, the giveaway was lavish indeed.

What's important to intellectual-property owners is simple: duration, duration, duration. That's why, when the expiration of a drug company's patent nears, we see the company scrambling shamelessly to propose dubious new, patentable uses for its lucrative products. A pharmaceutical maker will do anything to lengthen its exclusive hold on its drugs. In the realm of copyright, we see intellectual-property titleholders trying to earn royalties for longer periods.

This fall, the legal challenge to the Sonny Bono Act reached the U.S. Supreme Court. The case, *Eldred v. Ashcroft*, addresses a pressing intellectual-property issue—namely, how committed are we to the notion of the public domain? The case involves the right of Eric Eldred, a computer analyst and Internet hobbyist, to post pieces of literature—including *The Great Gatsby* by F. Scott Fitzgerald—whose copyrights would have expired were it not for Congress's intervention. Many of the works Eldred wants to make freely available at www.eldritchpress.org, his noncommercial Web site, are now out of print. Examples include *Horses and Men,* a collection of stories by Sherwood Anderson, and a rare edition of Robert Frost's *New Hampshire* poetry collection; both were published in 1923. The Sonny Bono law denies the public the chance to view these works on free sites; any such use or other copying would require paying royalties to the authors' estates.

Like patent rights, copyright is covered by Article 1 of the U.S. Constitution, which states that Congress shall have the authority "to promote the progress of science and useful arts, by securing *for limited times* [emphasis added] to authors and inventors the exclusive right to their respective writings and discoveries." Originally, Congress specified that copyright should last 14 years, renewable to no more than 28 years.

The idea was wise and simple: authors and inventors should be able to control rights to their works for a brief period during which they can reap the rewards. This encourages creativity and innovation. But to help disseminate these works widely, the works should revert to the public domain as soon as reasonably possible. That way the public benefits, too.

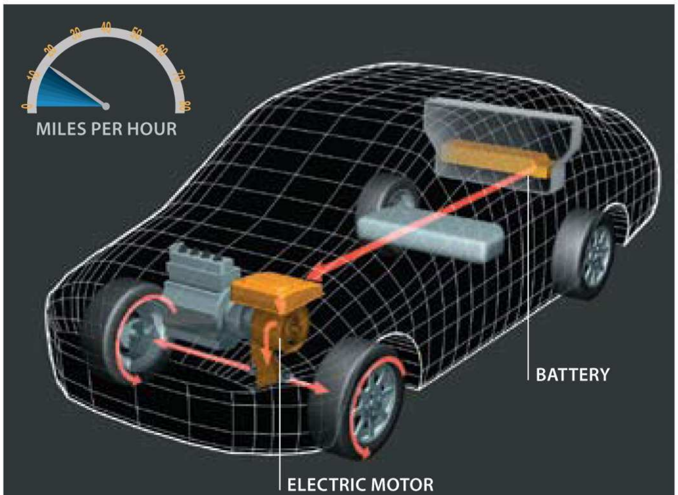
Lawrence Lessig, a Stanford University law professor, champion of the public domain, and the driving force behind the Eldred case, likes to remind people that the classic renderings of both Uncle Sam and Santa Claus were the work of Thomas Nast. We take them for granted now, but had the Sonny Bono Act been in place, everyone from the Department of Defense to department stores would have had to pay royalties. Neither image would likely be a feature of our public life.

Congress stole the public's access to its own cultural heritage by extending copyright protection to benefit a few big media companies. Fortunately, the public has the Constitution on its side.

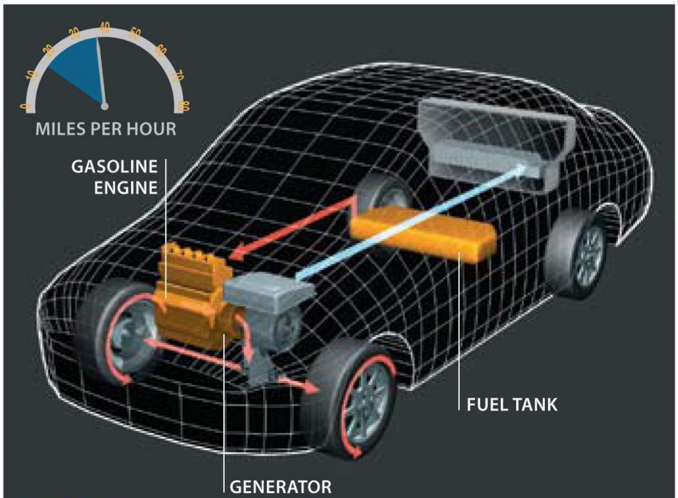
But all that was forgotten when the Mickey Mouse legislation was passed in October 1998. The public was thoroughly shut out of the process. There was virtually no open debate in the House or Senate, and President Clinton quietly signed this travesty into law. The lawmakers and Clinton knew they were robbing the public to enrich a few powerful corporate titleholders. They knew they were limiting the public's access to its own cultural heritage.

Thanks to the tireless work of people such as Lessig, the case is now before the U.S. Supreme Court. Eldred has been joined by some nine additional plaintiffs—organizations in the business of providing access to such public-domain works as songs, books, and films. Friend-of-the-court briefs in support of the plaintiffs have been filed by economists, intellectual-property law professors, no fewer than 15 library associations, and a bevy of well-known authors, including Peter Matthiessen.

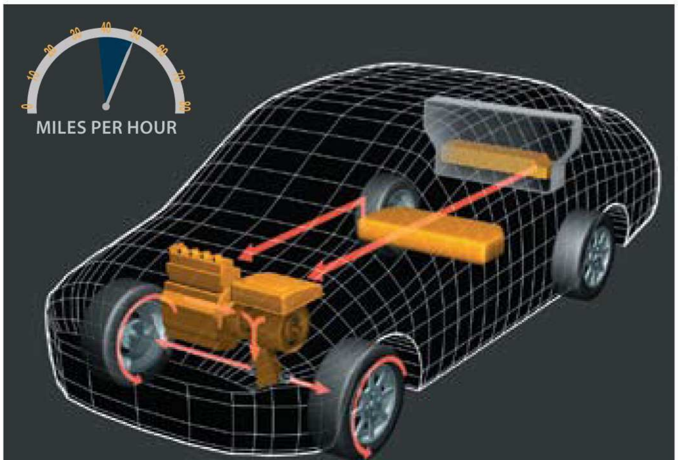
The Supreme Court's track record on copyright issues offers little to indicate how the justices might rule; indeed, most analysts were surprised the justices even agreed to hear the case. Copyright lawyers emphasize that a Supreme Court decision is likely to have profound implications for intellectual property. Whatever the outcome, the showdown shines a spotlight on a shameful corporate handout that ought to prompt us to reassert the public's part in the patent and copyright bargain.



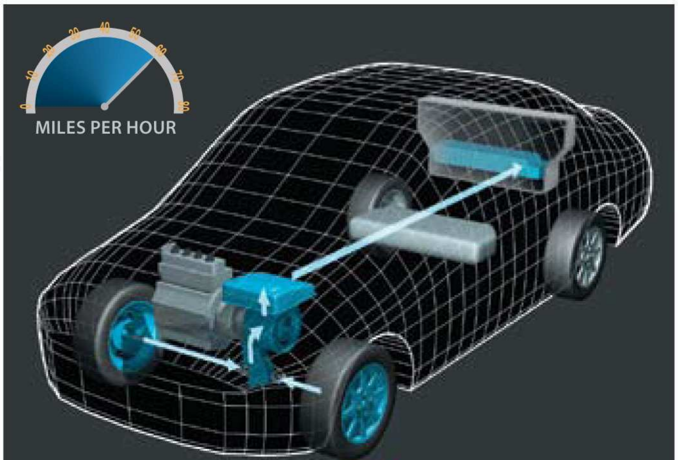
STARTING OUT
The electric motor powers the vehicle upon startup and at slow speeds, when the gasoline engine would be least efficient.



CRUISING
The gasoline engine drives the wheels and also sends power to the generator, which charges the battery.



PASSING
When extra load is placed on the car, such as during acceleration or hill climing, the gasoline engine and the electric motor work simultaneously.



SLOWING DOWN
When the driver decelerates and brakes, the wheels continue turning the motor, which switches into generator mode, converting kinetic energy into electricity to recharge the battery.

By Tracy Staedter | Illustration by John MacNeill

HYBRID CARS

Automakers have finally combined the best of two cars—the electric and the gasoline powered—into one fuel-efficient hybrid. The Honda Insight and the Toyota Prius *(above)*, which arrived in U.S. showrooms in 1999 and 2000, respectively, rely primarily on gasoline, switching to electricity under light loads, or use both types of energy simultaneously when the vehicle needs a boost of power. Sensors placed throughout the car monitor conditions such as throttle position, vehicle speed, and battery charge, and relay the readings to a computer that decides how to optimally divide the load between the gasoline engine and electric motor.

Neither the Insight nor the Prius needs to be plugged in; both recharge their battery during normal operation. One clever way they accomplish this is through regenerative braking. When the driver decelerates or brakes, the motion of the slowing wheels turns the generator and creates energy that is used to recharge the battery. By using the otherwise wasted energy of braking, the hybrids get better gas mileage in the city than conventional vehicles do. The Prius averages 48 miles per gallon, the Insight, 56 mpg. Both are rated by the California Air Resources Board as being 90 percent cleaner than the average new 2002 model year car. TR

For an animated version of this illustration, go to www.technologyreview.com/visualize

INDEX

PEOPLE AND ORGANIZATIONS MENTIONED IN THIS ISSUE

PEOPLE

ORGANIZATIONS

ANYWAY, ANYHOW, ANYWHERE

The first laptop went into space, but it brought computing down to earth

Laptop computers have become wildly popular in recent years. Their appeal lies in their portability: the light, compact computers can be taken anywhere, liberating busy people from the confines of their offices. Almost eight million PC laptops were sold in the United States last year, and according to Gartner, a market-research firm based in Stamford, CT, over the next four years, laptop sales will grow at approximately twice the rate of desktop computer sales. Yet the laptop's basic design hasn't changed much since it was created some two decades ago.

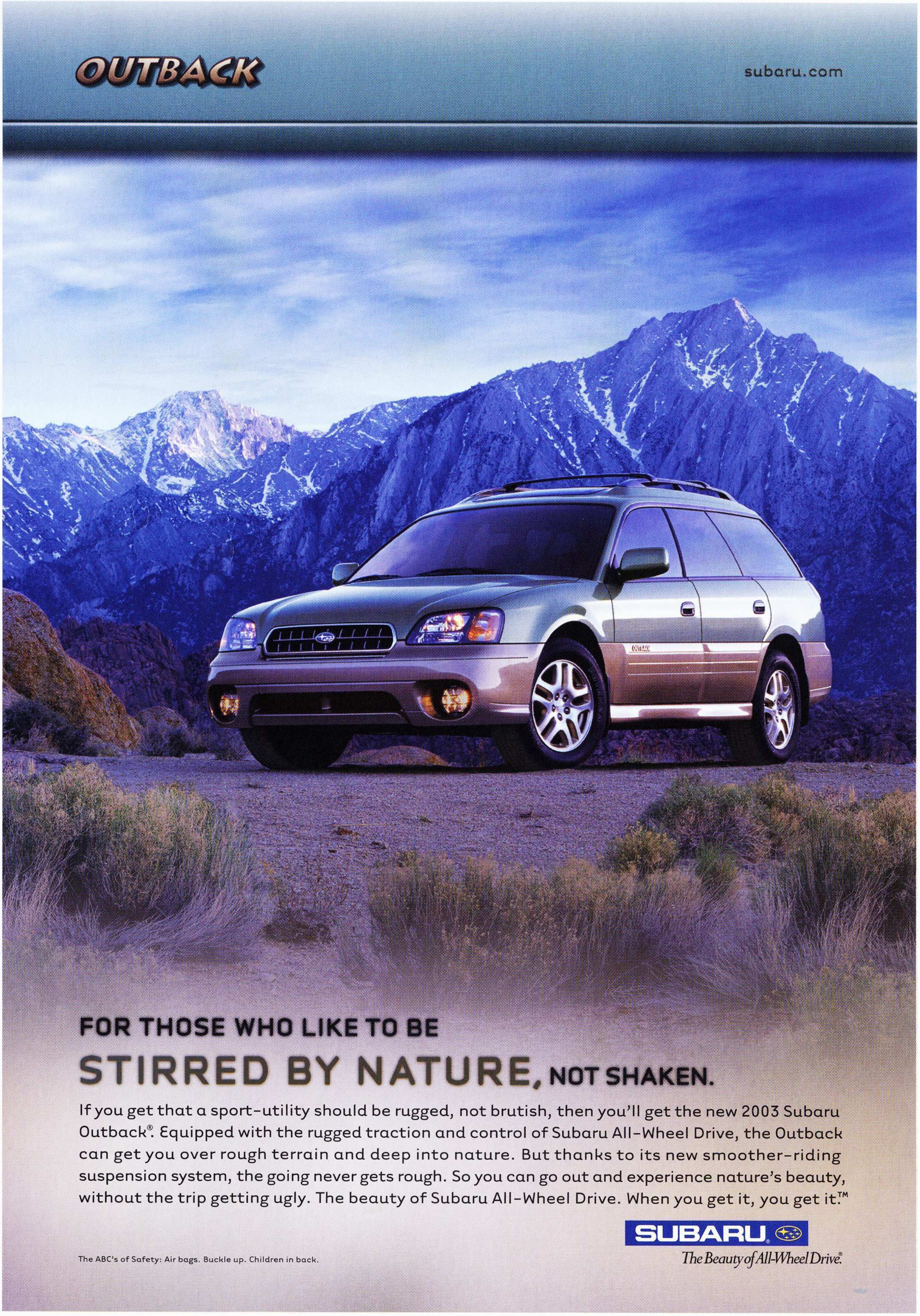
Back in the 1970s, when computers were anything but portable, Xerox Palo Alto Research Center (PARC) researcher Alan Kay conceived the initial idea for the laptop. He hashed out a design for a notebook-size portable computer he called the Dynabook. It was pure theory, however: the technology did not yet exist to make the Dynabook a reality, and Xerox was unwilling to fund development of the idea. But another Xerox PARC researcher, John Ellenby, decided to give the notebook-size computer a shot. In 1979 Ellenby founded his own company, GRiD Systems. He presented his idea to Bill Moggridge, of IDTwo, a San Francisco design firm. Moggridge and his team soon got to work, and in 1981 the Compass laptop *(above)* was born.

The Compass was bursting with innovative design ideas, most of which are taken for granted today. Although hefty by current standards, the eight-pound Compass was much lighter than desktop computers of the time. It had a built-in modem, thin-screen display, and protective metal casing. Its most influential feature by far, though, was its hinged design: when the computer was not in use, its screen could be folded over the keyboard, making the Compass compact and protecting it from damage. In fact, the design was so influential that GRiD Systems made some $7 million by licensing its design patents to other laptop makers such as Toshiba and Sanyo.

Later, Ellenby founded GeoVector, a San Francisco mobile-device technology company. Moggridge cofounded IDEO, the Palo Alto, CA, firm that designed the Handspring Treo, a cutting-edge personal digital assistant. On their heels other laptop makers would make advances, particularly in power supply design and wireless capability. But back in 1983 the Compass was far enough ahead of its time to be used by NASA on Space Shuttle missions: the Compass was the first PC to travel to outer space. Its influence on laptops today continues to be out of this world. —*David Rapp*

COURTESY OF IDEO

Technology Review (ISSN 1099-274X), Reg. U.S. Patent Office, is published monthly, except bimonthly in December/January and July/August, by the Massachusetts Institute of Technology. Entire contents ©2002. The editors seek diverse views, and authors' opinions do not represent the official policies of their institutions or those of MIT. Printed by Brown Printing Company, Waseca, MN. Periodicals postage paid at Boston, MA, and additional mailing offices. Postmaster: send address changes to *Technology Review*, Subscription Services Dept., PO Box 420005, Palm Coast, FL 32142 , or via the Internet at www.technologyreview.com/custserv/inquiry. Basic subscription rates: $34 per year, Canadian residents add $10, other foreign countries add $30. Publication Mail Agreement Number 40621028. Send undeliverable Canadian copies to PO Box 1051 Fort Erie, ON L2A 6C7. Printed in U.S.A.
ABC audited


OUTBACK
subaru.com
FOR THOSE WHO LIKE TO BE
STIRRED BY NATURE, NOT SHAKEN.
If you get that a sport-utility should be rugged, not brutish, then you'll get the new 2003 Subaru Outback®. Equipped with the rugged traction and control of Subaru All-Wheel Drive, the Outback can get you over rough terrain and deep into nature. But thanks to its new smoother-riding suspension system, the going never gets rough. So you can go out and experience nature's beauty, without the trip getting ugly. The beauty of Subaru All-Wheel Drive. When you get it, you get it.™
SUBARU
The Beauty of All-Wheel Drive.®
The ABC's of Safety: Air bags. Buckle up. Children in back.